UNIVERSIDADE FEDERAL DE RONDONÓPOLIS

REITORIA
DIRETORIA DE GABINETE-REITORIA

CONTRATO Nº 2/2025

Processo nº 23853.012662/2024-72

Unidade Gestora: **156677**

CONTRATO ADMINISTRATIVO Nº 02/2025, QUE FAZEM ENTRE SI A UNIVERSIDADE FEDERAL DE RONDONÓPOLIS E A EMPRESA ADVANTA SISTEMAS DE TELECOMUNICAÇÕES E SERVIÇOS DE INFORMÁTICA LTDA.

A **UNIVERSIDADE FEDERAL DE RONDONÓPOLIS**, com sede na Avenida dos Estudantes, nº 5055, Bairro Cidade Universitária, na cidade de Rondonópolis/MT, inscrita no CNPJ/MF sob o nº 35.854.176/0001-95, neste ato representada pela sua Reitora Profª. **ANALY CASTILHO POLIZEL DE SOUZA**, nomeada pelo Decreto Presidencial de 26 de dezembro de 2023, publicado no DOU de 27 de dezembro de 2023, portadora da matrícula funcional nº 1493862, doravante denominado CONTRATANTE, e a **ADVANTA SISTEMAS DE TELECOMUNICAÇÕES E SERVIÇOS DE INFORMÁTICA LTDA** , inscrita no CNPJ/MF sob o nº 03.232.670/0001-21, sediada no Município de Barueri, Estado de São Paulo, na Avenida Copacabana, nº 325, Empresarial 18 do Forte, Salas 1810 a 1814 - CEP 06472-001, doravante designado CONTRATADO, neste ato representada por **RAFAEL ALVES DE SOUZA** , sócio, conforme atos constitutivos da empresa, tendo em vista o que consta no Processo nº 23853.012662/2024-72 e em observância às disposições da Lei nº 14.133, de 1° de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente da Ata de Registro de Preços oriunda do Pregão Eletrônico nº 31009/2023 do Instituto Federal de Santa Catarina, mediante as cláusulas e condições a seguir enunciadas.

1. **CLÁUSULA PRIMEIRA – OBJETO (ART. 92, I E II)**

1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação composta por AQUISIÇÃO DE EQUIPAMENTOS DE SEGURANÇA DE TI, nas condições estabelecidas no Termo de Referência.

1.2. Este instrumento contratual tem por objeto os serviços vinculados aos bens móveis descritos no item 1.3.

São serviços vinculados:

1.2.0.1. Entrega dos equipamentos;

1.2.0.2. Instalação/configuração dos equipamentos;

1.2.0.3. Abertura de chamados - recebimento por parte da contratada;

1.2.0.4. Atendimento de um chamado aberto;

1.2.0.5. Resolução total de um problema apresentado em um chamado.

Os serviços vinculados descritos acima, serão avaliados mediante os instrumentos de medição disponíveis no Termo de Referência.

1.3. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
01	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 5 - FC-10-F200F-950-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 2. Marca: SEM, Fabricante: SEM	UNIDADE	01	R$ 63.288,89	R$ 63.288,89
02	SERVIÇO DE SUPORTE E GARANTIA SWITCH CORE - TIPO 1 - FC-10-S424I-247-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 2. Marca: FORTINET, Fabricante: FORTINET	UNIDADE	01	R$ 4.329,65	R$ 4.329,65
	Código: 44905237001000090 SWITCH CORE - TIPO 1 – SOLUÇÃO DE SEGURANÇA DE DADOS Características Mínimas: 1.1 Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;				

	1.2 Deve possuir 24 (vinte e quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE; 1.3 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; 1.4 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; 1.5 Deve possuir 1 (uma) interface USB; 1.6 Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 200 Mpps (milhões de pacotes por segundo); 1.7 Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 1.8 Deve possuir tabela MAC com suporte a 32.000 endereços; Deve operar com latência igual ou inferior à 1us (microsegundo); 1.9 Deve implementar Flow Control baseado no padrão IEEE 802.3X; 1.10 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; 1.11 Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 1.12 Deve suportar MultiChassis 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 switches como uma única interface lógica; 1.13 Deve suportar a comutação de Jumbo Frames; 1.14 Deve identificar automaticamente telefones IP que estejam conectados e associá- los automaticamente a VLAN de voz; 1.15 Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 1.16 Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 1.17 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; 1.18 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 exiga licenciamento adicional para ativação do protocolo; 1.19 Deverá suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo; 1.20 Deve implementar serviço de DHCP Server e DHCP Relay; 1.21 Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos; 1.22 Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN); 1.23 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; 1.24 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; 1.25 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; 1.26 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; 1.27 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; 1.28 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; 1.29 Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O				

03	switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 1.30 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; 1.31 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; 1.32 Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 1.33 Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 1.34 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; 1.35 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); 1.36 Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 1.37 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; 1.38 Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement; 1.39 Deverá implementar mecanismo de proteção contra ataques do tipo man-in-themiddle que utilizam o protocolo ARP; 1.40 Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 1.41 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; 1.42 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; 1.43 Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 1.44 Deve suportar MAC Authentication Bypass (MAB); 1.45 Deve implementar RADIUS CoA (Change of Authorization); 1.46 Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 1.47 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; 1.48 Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 1.49 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; 1.50 Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 1.51 Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 1.52 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; 1.53 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); 1.54 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; 1.55 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;	UNIDADE	01	R$ 27.268,29	R$ 27.268,29

	1.56 Deve suportar o protocolo PTP (Precision Time Protocol); 1.57 Deve implementar Netflow, sFlow ou similar; 1.58 Deve suportar o envio de mensagens de log para servidores externos através de syslog; 1.59 Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 1.60 Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 1.61 Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 1.62 Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 1.63 Deve permitir ser gerenciado através de IPv6; 1.64 Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 1.65 Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 1.66 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; 1.67 Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 1.68 Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 1.69 Deverá suportar ser configurado e monitorado através de REST API; 1.70 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; 1.71 Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash; 1.72 Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 1.73 Deve suportar temperatura de operação de até 45º Celsius; 1.74 Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 1.75 Deve ser fornecido com fontes de alimentação redundantes e internas ao equipamento, com capacidade para operar em tensões de 110V e 220V; 1.76 Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. 1.78 Todos os acessórios para montagem e fixação deverão ser fornecidos; 1.79 Marca: FORTINET, Fabricante: FORTINET.				
	Código: 44905237001000103 SOLUÇÃO DE SEGURANÇA DE DADOS - 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, 15 (quinze) interfaces 1 Gigabit Ethernet padrão 1000Base-T e 4 (quatro) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Adicionalmente devem ser fornecidos 2 (dois) transceivers SFP+ conforme padrão 10GBase-SR; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação redundante com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. Deve suportar a instalação de fonte de alimentação redundante; 7. 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; 8. Quaisquer licenças e/ou softwares necessários para plena execução de todas as				

características descritas neste termo de referência deverão ser fornecidos;

9. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo;

10. 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;

11. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

12. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica;

13. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso;

14. 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;

15. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;

16. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 3072 (três mil e setenta e dois) portas de switch ou um total de 64 (sessenta e quatro) switches;

17. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas;

18. A solução deve permitir, através da interface gráfica, configurar VLANs e distribui-las automaticamente nos switches e pontos de acesso por ela gerenciados;

19. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

20. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

21. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

22. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

23. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

24. 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;

25. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;

26. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;

27. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 128 (cento e vinte e 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;

28. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b /g/n/ac/ax;

29. 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;

30. 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;

31. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6;

32. 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;

33. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

34. 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;

35. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de lista 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;

36. 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;

37. 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;

38. 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;

39. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos;

40. A solução deverá ser capaz de encaminhar 13 Gbps de tráfego encapsulado via VPN IPSec;

41. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

42. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard);

43. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

44. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs;

45. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec;

46. A solução deverá ser capaz de atuar como um cliente de VPN SSL;

47. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

48. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL;

49. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar;

50. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

51. 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;

52. 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;

53. 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;

54. 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;

55. 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;

56. 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; 57. 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; 58. 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; 59. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 60. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 61. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 62. 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; 63. 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; 64. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 65. 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; 66. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 67. 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; 68. 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; 69. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 70. 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; 71. A solução deve permitir a configuração dos parâmetros BLE (Blueooth Low Energy) nos pontos de acesso; 72. 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; 73. 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; 74. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 75. 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; 76. 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; 77. 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; 78. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os				

	seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI.				
04	79. 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; 80. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 81. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 82. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 83. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 84. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 85. 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; 86. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAPTTLS e PEAP; 87. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 88. A solução deverá suportar SingleSign-On (SSO); 89. 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; 90. 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; 91. 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; 92. 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 informar as credenciais válidas para acesso à rede; 93. 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; 94. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 95. A solução deve permitir a configuração do captive portal com endereço IPv6; 96. 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; 97. 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; 98. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 99. 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; 100. 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; 101. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 102. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 103. A solução deverá ser capaz de inspecionar 4 Gbps de tráfego SSL; 104. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;	UNIDADE	01	R$ 50.307,19	R$ 50.307,19

105. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 106. 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; 107. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 108.A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 109. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 110. 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; 111. 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; 112. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 113. 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; 114. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 115. 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; 116. 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; 117. A solução deverá ser capaz de tratar 13 Gbps de tráfego por meio do filtro de aplicações; 118. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 119. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 120. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 121. A solução deverá permitir a criação manual de novos padrões de aplicações; 122. 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; 123. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 124. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 125. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 126. 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; 127. 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; 128. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 129. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 130. A solução deverá ser capaz de tratar 27 Gbps de tráfego por meio das regras de firewall stateful 512 byte; 131. A solução deverá ser capaz de suportar 3.000.000 (três milhões) de sessões simultâneas/concorrentes e 280.000 (duzentos e oitenta mil) novas sessões por				

	segundo; 132. 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; 133. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 134. A solução deverá suportar PBR – Policy Based Routing; 135.A solução deverá suportar roteamento multicast; 136. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 137. A solução deverá possuir mecanismo de tratamento para aplicações multimidia (session-helpers ou ALGs) tipo SIP e H323; 138. A solução deverá possuir suporte à criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 139. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 140. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 141. 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; 142. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 143. 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; 144. 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; 145. 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; 146. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 147. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDPEcho. 148. 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; 149. 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). 150. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 151. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 152. 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; 153. 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; 154. 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; 155. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 156. A solução deverá suportar Netflow ou sFlow; 157. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 158. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS;				

	159. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 160. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 161. A solução deve permitir a captura de pacotes e exporta-los em arquivos com formato .pcap; 162. A solução deve possuir ferramentas de diagnósticos e debug 163. 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; 164. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 165. A solução deve suportar comunicação com elementos externos através de REST API; 166. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 167. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 168. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: 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). 169. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 170. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo. 171. Marca: FORTINET, Fabricante: FORTINET.				
	Código: 44905237001000092 SWITCH CORE TIPO 3 – SOLUÇÃO DE SEGURANÇA DE DADOS Características Mínimas: 1.01 Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 1.02 Deve possuir 24 (vinte e quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE; 1.03 Adicionalmente, deve possuir ao menos 2 (dois) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet; 1.04 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; 1.05 Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45; 1.06 Deve possuir capacidade de comutação de pelo menos 880 Gbps e ser capaz de encaminhar até 1200 Mpps (Milhões de pacotes por segundo); 1.07 Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 1.08 Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame conforme padrão IEEE 802.1ad; 1.09 Deve possuir tabela MAC com suporte a 60.000 endereços; 1.10 Deve implementar Flow Control baseado no padrão IEEE 802.3X; 1.11 Deve suportar o padrão IEEE 802.1Qbb (Prioritybased Flow Control); 1.12 Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 1.13 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 switches como uma única interface lógica; 1.14 Deve suportar a comutação de Jumbo Frames; 1.15 Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;				

	1.16 Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 1.17 Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos; 1.18 Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos; 1.19 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 exiga licenciamento adicional para ativação do protocolo; 1.20 Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo; 1.21 Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação deste recurso; 1.22 Deve permitir configurar determinadas portas físicas do switch como interfaces de camada 3 que tenha suporte às funções de roteamento sem requerer a configuração de uma VLAN; 1.23 Deve implementar serviço de DHCP Server e DHCP Relay; 1.24 Deve suportar o protocolo Virtual Extensible LAN (VXLAN) para permitir que o tráfego de camada 2 seja encaminhado para outros locais da rede via roteamento; 1.25 Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos; 1.26 Deve suportar o protocolo Multicast Listener Discovery (MLD) Snooping para otimizar as comunicações multicast em IPv6; 1.27 Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN); 1.28 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; 1.29 Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree; 1.30 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; 1.31 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; 1.32 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; 1.33 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; 1.34 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; 1.35 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; 1.36 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; 1.37 Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 1.38 Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 1.39 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; 1.40 Deverá implementar ao menos 1 (um) dos seguintes mecanismos de				
05		UNIDADE	01	R$ 162.169,45	R$ 162.169,45

	prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ); 1.41 Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 1.42 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; 1.43 Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement; 1.44 Deverá implementar mecanismo de proteção contra ataques do tipo man-in-themiddle que utilizam o protocolo ARP; 1.45 Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 1.46 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; 1.47 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; 1.48 Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 1.49 Deve suportar MAC Authentication Bypass (MAB); 1.50 Deve implementar RADIUS CoA (Change of Authorization); 1.51 Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 1.52 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; 1.53 Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 1.54 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; 1.55 Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 1.56 Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 1.57 Deve suportar MACSec para proteger e cifrar a comunicação entre switches; 1.58 Deve suportar o protocolo PTP (Precision Time Protocol); 1.59 Deve implementar Netflow, sFlow ou similar; 1.60 Deve suportar o envio de mensagens de log para servidores externos através de syslog; 1.61 Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 1.62 Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 1.63 Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 1.64 Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 1.65 Deve permitir ser gerenciado através de IPv6; 1.66 Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 1.67 Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 1.68 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; 1.69 Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 1.70 Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 1.71 Deverá suportar ser configurado e monitorado através de REST API; 1.72 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; 1.73 Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash; 1.74 Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 1.75 Deve suportar temperatura de operação de até 40º Celsius; 1.76 Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 1.77 Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V; 1.78 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; 1.79 GARANTIA E SUPORTE: Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;				
		VALOR TOTAL			**R$ 307.363,47**

1.4. Vinculam esta contratação, independentemente de transcrição:

O Termo de Referência;

O Edital da Licitação;

A Proposta do contratado;

Eventuais anexos dos documentos supracitados.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação estará vinculado ao período de garantia dos bens que serão adquiridos, de acordo com o exposto no Termo de Referência, a saber:

3 (três) anos para os demais itens.

2.2. Não haverá prorrogação de contrato.

3. CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (ART. 92, IV, VII E XVIII)

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

4. CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

5. CLÁUSULA QUINTA - PREÇO

5.1. O valor da execução dos serviços de instalação/configuração, bem como os serviços de suporte e garantia estão definidos como valores únicos não havendo ônus contínuo (mensal) para o IFSC.

5.2. No valor do equipamento estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6. CLÁUSULA SEXTA - PAGAMENTO (ART. 92, V E VI)

6.1. O prazo para pagamento (bens/serviços) ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

7. CLÁUSULA SÉTIMA - REAJUSTE (ART. 92, V)

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data da assinatura da Ata de Registro de Preços.

7.2. Após o interregno de um ano, considerando a renovação da Ata de Registro de Preços, os preços iniciais serão reajustados a pedido da Contratada, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.3. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.4. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

7.5. O reajuste será realizado por apostilamento.

8. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (ART. 92, X, XI E XIV)

8.1. São obrigações do Contratante, além das previstas no termo de referência: Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado; impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

A Administração terá o prazo de um mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

Responder eventuais pedidos de restabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de dois meses.

Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

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

9. CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (ART. 92, XIV, XVI E XVII)

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, além das previstas no termo de referência:

Entregar o objeto acompanhado do manual do usuário, com uma versão em português ou inglês, e a relação da rede de assistência técnica autorizada;

Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o código de defesa do consumidor (lei nº 8.078, de 1990);

Comunicar ao 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;

Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, ii, da lei n.º 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

Quando não for possível a verificação da regularidade no sistema de cadastro de fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a nota fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à seguridade social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) certidão negativa de débitos trabalhistas – CNDT;

Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;

Comunicar ao fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.

Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da previdência social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da lei n.º 14.133, de 2021);comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da lei n.º 14.133, de 2021);

Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da lei nº 14.133, de 2021);

Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, ii, d, da lei nº 14.133, de 2021.

Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante;

A empresa contratada deverá assinar o termo de compromisso de manutenção de sigilo e o termo de ciência da declaração de manutenção de sigilo resguardando que os recursos, dados e informações de propriedade da contratante, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, que constituam informação privilegiada e possuem caráter de confidencialidade.

10. CLÁUSULA DÉCIMA PRIMEIRA – OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a Lei no 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6° da LGPD.

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

10.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

10.11. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

10.12. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

10.13. Os contratos e convênios de que trata o §1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

11. CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (ART. 92, XII)

11.1. Não haverá exigência de garantia contratual da execução.

12. CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (ART. 92, XIV)

12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

i) Não atender os prazos estipulados no Termo de Referência para os serviços vinculados.

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

i. **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

ii. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas "b", "c","d" e "i" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, bem como nas alíneas "b", "c", "d" e "i", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

iv. **Multa:**

1. moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor unitário licitado do bem ao qual foi acionada a garantia, até o limite de 10 (dez) dias;
2. Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 11.1, de 2% a 5% do valor do Contrato;.
3. Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 11.1, de 3% a 6% do valor do Contrato.
4. Para infração descrita na alínea "b" do subitem 11.1, a multa será de 4% a 7% do valor do Contrato.
5. Para infrações descritas na alínea "d" do subitem 11.1, a multa será de 5% a 8% do valor do Contrato.
6. Para a infração descrita na alínea "a" do subitem 11.1, a multa será de 5% a 8% do valor do Contrato, ressalvadas as seguintes infrações:

i. Para a infração descrita na alínea "i" do subitem 11.1, a multa será a descrita no termo de referência, nos instrumentos de medição.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e

contratar e de declaração de inidoneidade para licitar ou contratar.

12.6. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;
b) as peculiaridades do caso concreto;
c) as circunstâncias agravantes ou atenuantes;
d) os danos que dela provierem para o Contratante;
e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.7. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

12.8. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

12.9. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

12.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

12.11. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

13. CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (ART. 92, XIX)

13.1. O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

13.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:

a) ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

b) poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

13.3. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.3.0.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.4. O termo de extinção, sempre que possível, será precedido:

Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;
Relação dos pagamentos já efetuados e ainda devidos;
Indenizações e multas.

13.5. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

13.6. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

14. CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA (ART. 92, VIII)

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

I. Gestão/Unidade: 156993
II. Fonte de Recursos: 300800 e 100000
III. Programa de Trabalho: 231301
IV. Elemento de Despesa: 449052 e 339052
V. Plano Interno: VETICN9900N

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS (ART. 92, III)

15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

16.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria

jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

17. CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

18. CLÁUSULA DÉCIMA OITAVA – FORO (ART. 92, §1º)

18.1. Fica eleito o Foro da Subseção Judiciária de Rondonópolis - MT, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Rondonópolis, 13 de janeiro de 2025.

_____

UNIVERSIDADE FEDERAL DE RONDONÓPOLIS

ANALY CASTILHO POLIZEL DE SOUZA

Representante Legal da CONTRATANTE

_____

ADVANTA SISTEMAS DE TELECOMUNICAÇÕES E SERVIÇOS DE INFORMÁTICA LTDA

RAFAEL ALVES DE SOUZA

Representante Legal da CONTRATADA

Documento assinado eletronicamente por **Analy Castilho Polizel de Souza**, **Reitor(a) da Universidade Federal de Rondonópolis - REITORIA/UFR**, em 13/01/2025, às 18:02, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **RAFAEL ALVES DE SOUZA**, **Usuário Externo**, em 14/01/2025, às 09:27, conforme horário oficial de Brasília, com fundamento no art. 6º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufr.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0450303** e o código CRC **6E8C89D5**.