COTAÇÃO ELETRÔNICA - AQUISIÇÃO DE HARDWARE DE REDE E CONFIGURAÇÃO DA SOLUÇÃO

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1. OBJETO

O presente documento tem por objeto a contratação de solução Cisco Meraki completa para o refresh tecnológico da infraestrutura de rede de dados, abrangendo rede cabeada e rede sem fio, com fornecimento de equipamentos, licenciamento, serviços profissionais de implantação, testes, documentação técnica e suporte à entrada em operação.

A solução deverá contemplar arquitetura moderna, escalável e de alta disponibilidade, incluindo plataforma de gestão e automação operacional de rede, controle de acesso à rede corporativa baseado em identidade e plataforma de inteligência, analytics e experiência sobre a rede wireless, observando rigorosamente a segregação lógica entre rede corporativa e rede de visitantes.

O escopo compreende ainda a adequação da infraestrutura às boas práticas do fabricante, bem como o atendimento a requisitos de segurança, rastreabilidade, auditoria e governança, garantindo previsibilidade contratual e clareza de responsabilidades entre Contratante e Contratada.

2. OBJETIVO

2.1 Objetivo Geral:

Estabelecer os requisitos técnicos necessários para a contratação de solução de infraestrutura de rede que assegure desempenho, segurança, escalabilidade, padronização operacional e governança, alinhada às boas práticas do fabricante e às necessidades atuais e futuras da organização.

2.2 Objetivo Específicos:

- Modernizar a infraestrutura de rede cabeada e wireless, adotando arquitetura hierárquica e equipamentos compatíveis com elevados níveis de disponibilidade e crescimento futuro.
- Centralizar a gestão da infraestrutura por meio de plataforma de gestão e automação operacional de rede, garantindo visibilidade, automação de rotinas e simplificação da operação.
- Implementar conectividade wireless segura, mantendo segregação lógica completa entre rede corporativa e rede de visitantes.
- Adotar controle de acesso à rede corporativa baseado em identidade, por meio de autenticação, autorização e contabilização (AAA clássico), utilizando IEEE 802.1X e MAB.

- Utilizar plataforma de inteligência, analytics e experiência sobre a rede wireless para coleta, correlação e análise de eventos da rede Wi-Fi, com aplicação restrita às funcionalidades relevantes ao ambiente.
- Garantir rastreabilidade, auditoria e visibilidade operacional das conexões, sem interferência no plano de dados.

3. ESCOPO DA CONTRATAÇÃO

O escopo da contratação compreende:

- Fornecimento de todos os equipamentos de rede especificados nesta especificação técnica, incluindo switches, access points e acessórios necessários ao pleno funcionamento da solução.
- Fornecimento de licenciamento de software e serviços em nuvem pelo período definido contratualmente.
- Implantação lógica da solução, incluindo configuração, integração entre componentes, testes e validação.
- Execução de serviços profissionais especializados, incluindo planejamento, implantação, testes funcionais e site survey ativo para validação da rede wireless.
- Elaboração e entrega de documentação técnica completa da solução implantada.

Não fazem parte do escopo:

- Fornecimento de infraestrutura física e virtualização;
- Desenvolvimento de integrações customizadas fora do escopo definido;
- Funcionalidades avançadas explicitamente excluídas nos capítulos específicos.

4. PREMISSAS TÉCNICAS GERAIS

A solução deverá observar as seguintes premissas técnicas:

- Operação com separação clara entre plano de controle e plano de dados, garantindo que plataformas de gestão não interfiram no tráfego dos usuários.
- Segregação lógica completa entre rede corporativa e rede de visitantes, em todas as camadas da arquitetura.
- Utilização exclusiva de tecnologias suportadas e recomendadas pelo fabricante.
- Adoção de arquitetura escalável, permitindo expansão futura sem redesign estrutural.

- Clareza de escopo funcional, com exclusão explícita de funcionalidades não exigidas, evitando sobreposição entre plataformas.

5. ESTRUTURA TÉCNICA DA SOLUÇÃO

A solução deverá ser estruturada de forma modular e hierárquica, contemplando:

- Camada de Core, responsável pela comutação e roteamento central da rede.
- Camada de Distribuição, responsável pela agregação da camada de acesso em áreas específicas.
- Camada de Topo de Rack (ToR), destinada à agregação de servidores.
- Camada de Acesso, responsável pela conexão de dispositivos finais e access points.
- Camada Wireless, baseada em access points Wi-Fi de última geração.
- Plataforma de Gestão e Automação Operacional de Rede, responsável pela gestão, visibilidade e automação operacional.
- Solução de Controle de Acesso à Rede (NAC), responsável pelo controle de acesso corporativo baseado em identidade.
- Plataforma de Inteligência, Analytics e Experiência sobre a Rede Wireless, utilizada para visibilidade e rastreabilidade do ambiente.

Cada componente deverá possuir papel bem definido, sem sobreposição funcional, garantindo coerência arquitetural e previsibilidade operacional.

6. ESPECIFICAÇÕES DE HARDWARE

As especificações a seguir definem os requisitos mínimos de hardware para o processo de aquisição de hardware de rede e configuração.

Os equipamentos deverão atender plenamente às necessidades de desempenho, confiabilidade e compatibilidade com as ferramentas utilizadas pela FUNDAÇÃO, garantindo suporte às atividades diárias com eficiência e segurança.

Item	Descrição	Group Name	Qtdade
C9300X-24Y-M	C9300X 24x25GE SFP+, 715wac PS, w/MERAKI	CORE	4

LIC-C9300-24E-5Y	Meraki Enterprise License for C9300-M 24-port, 5 year	CORE	4
PWR-C1-715WAC-P-M	C9000 715W AC Platinum Power Supply, w/MERAKI	CORE	4
C9300X-NM-2C-M	C9300X 2-port 40G/100G SFP+ Network Module, w/MERAKI	CORE	4
STACK-T1-50CM-M	C9000 50CM Type 1 Stacking Cable, w/MERAKI	CORE	3
STACK-T1-1M-M	C9000 1M Type 1 Stacking Cable, w/MERAKI	CORE	1
CAB-SPWR-30CM-M	C9000 Stack Power Cable 30 CM, w/MERAKI	CORE	3
CAB-SPWR-150CM-M	C9000 Stack Power Cable 150 CM, w/MERAKI	CORE	1
CAB-ACBZ-10A	AC Power Cord (Brazil) 10A/250V BR-3-10 plug up to 10A	CORE	4
C9300X-24Y-M	C9300X 24x25GE SFP+, 715wac PS, w/MERAKI	DISTRI + ToR	3
LIC-C9300-24E-5Y	Meraki Enterprise License for C9300-M 24-port, 5 year	DISTRI + ToR	3
PWR-C1-715WAC-P-M	C9000 715W AC Platinum Power Supply, w/MERAKI	DISTRI + ToR	3
C9300X-NM-2C-M	C9300X 2-port 40G/100G SFP+ Network Module, w/MERAKI	DISTRI + ToR	3
STACK-T1-50CM-M	C9000 50CM Type 1 Stacking Cable, w/MERAKI	DISTRI + ToR	3
CAB-SPWR-30CM-M	C9000 Stack Power Cable 30 CM, w/MERAKI	DISTRI + ToR	3
CAB-ACBZ-10A=	AC Power Cord (Brazil) 10A/250V BR-3-10 plug up to 10A	DISTRI + ToR	3
MS150-48MP-4X	Meraki MS150-48MP-4X Cld-Mngd 32GE + 16(5GE) 740W PoE Switch	ACCESS	70
LIC-MS150-48-5Y	Meraki MS150-48 Enterprise License and Support, 5 Year	ACCESS	70
MA-CBL-100G-50CM	Meraki 100GbE QSFP Cable, 0.5 Meter	ACCESS	70
MA-PWR-CORD-BR	Meraki AC Power Cord for MX and MS (Brazil Plug)	ACCESS	70
CW9172I-RTG	Cisco Wireless 9172I(W7,3 radio,3 band 2x2),Global	WLAN	330
CW9176I-RTG	Cisco Wireless 9176I(W7,3 radio,3 band 4x4,UWB),Global	WLAN	25
LIC-MR-ADV-5Y	Meraki MR Advanced License and Support, 5YR	WLAN	355
R-ISE-VMC-K9=	Cisco ISE Virtual Machine Common PID	NAC	2
CON-L1SW-RISE9KVM	ENH SW Cisco ISE Virtual Ma	NAC	2
ISE-SEC-SUB	Cisco Identity Service Engine Subscription	NAC	1
ISE-E-LIC	Cisco Identity Service Engine Essentials Subscription	NAC	1500
SVS-ISE-SUP-B	Cisco Support Standard for ISE	NAC	1
40GBase-LR4 QSFP+	(SMF 1270nm to 1330nm, 10km, LC, DOM)	SFP	8
10GBase-LR SFP+	(SMF 1310nm, 10km, LC, DOM)	SFP	152

7. DETALHAMENTO DA ARQUITETURA DE REDE

7.1. **SWITCH CORE**

Responsáveis pela comutação e roteamento central da rede, agregando todas as camadas, garantindo alta disponibilidade, desempenho máximo, convergência rápida e políticas globais de rede.

Modelo considerado: Cisco Catalyst 9300X-24Y-M ou superior.

Características mínimas:

- Empilhamento físico entre os switches.

- Fontes redundantes hot-swap.
- Módulo de uplink com 2 interfaces 40/100G QSFP28.
- Conectividade:
    - 40 Gbps para switches de Distribuição.
    - 10 Gbps para switches de Acesso.

Arquitetura de hardware:

- 24 portas SFP28 por equipamento
- Suporte nativo a 1G, 10G e 25G
- Capacidade mínima de comutação por equipamento: 2.000 Gbps
- Capacidade de encaminhamento mínima: 1.488 milhões de pacotes por segundo (Mpps)

Empilhamento (Stacking):

- Empilhamento físico por portas dedicadas de hardware
- Capacidade mínima de empilhamento: 1 Tbps por stack
- Suporte para 8 switches por pilha

Uplink e Downlinks:

- 2 portas QSFP28
- Suporte a 40G e 100G

Alta disponibilidade e Energia:

- Fontes de alimentação redundantes hot-swap
- Ventiladores hot-swap
- Suporte a StackPower
- Operação contínua mesmo em falha de fonte ou ventilador

Funcionalidades de Camada de rede:

- Layer 2 avançado: IEEE 802.1Q (VLAN tagging), MSTP (802.1s) e RSTP Proteções de STP, Link Aggregation (LACP), IGMP Snooping, Storm Control (broadcast, multicast e unicast desconhecido), LLDP e CDP.

- Layer 3: Static Routing, OSPFv2, VRRP / Warm Spare, Multicast PIM-SM, DHCP Server e DHCP Relay.

Segurança

- IEEE 802.1X
- MAB (MAC Authentication Bypass)
- ACL IPv4 e IPv6 em hardware
- DHCP Snooping
- Dynamic ARP Inspection
- Port Security

7.2. **SWITCH TOPO DE HACK (ToR)**

Responsáveis pela agregação de servidores e equipamentos de infraestrutura em data center, oferecendo alta capacidade de throughput e baixa latência para tráfego leste-oeste e norte-sul.

Modelo considerado: Cisco Catalyst 9300X-24Y-M ou superior.

Características mínimas:

- Empilhamento físico entre os switches.
- Fontes redundantes hot-swap.
- Módulo de uplink com 2 interfaces 40/100G QSFP28.
- Uplinks de 40 Gbps para os Switches de Core.

Arquitetura de hardware:

- 24 portas SFP28 por equipamento
- Suporte nativo a 1G, 10G e 25G
- Capacidade mínima de comutação por equipamento: 2.000 Gbps
- Capacidade de encaminhamento mínima: 1.488 milhões de pacotes por segundo (Mpps)

Empilhamento (Stacking):

- Empilhamento físico por portas dedicadas de hardware
- Capacidade mínima de empilhamento: 1 Tbps por stack
- Suporte para 8 switches por pilha

Uplink e Downlinks:

- 2 portas QSFP28
- Suporte a 40G e 100G

Alta disponibilidade e Energia:

- Fontes de alimentação redundantes hot-swap
- Ventiladores hot-swap
- Suporte a StackPower
- Operação contínua mesmo em falha de fonte ou ventilador

Funcionalidades de Camada de rede:

- Layer 2 avançado: IEEE 802.1Q (VLAN tagging), MSTP (802.1s) e RSTP Proteções de STP, Link Aggregation (LACP), IGMP Snooping, Storm Control (broadcast, multicast e unicast desconhecido), LLDP e CDP.
- Layer 3: Static Routing, OSPFv2, VRRP / Warm Spare, Multicast PIM-SM, DHCP Server e DHCP Relay.

Segurança

- IEEE 802.1X
- MAB (MAC Authentication Bypass)
- ACL IPv4 e IPv6 em hardware
- DHCP Snooping
- Dynamic ARP Inspection
- Port Security

7.3. **SWITCH DISTRIBUIÇÃO**

Responsáveis pela agregação dos switches de acesso, aplicação de políticas de segmentação e encaminhamento otimizado do tráfego entre a camada de acesso e o core.

Modelo considerado: Cisco Catalyst 9300X-24Y-M

Características mínimas:

- Empilhamento em pares (3 pilhas distintas).
- Fontes redundantes hot-swap.
- Módulo de uplink com 2 portas 40/100G QSFP28.

- Conectividade:
    - 40 Gbps para Core.
    - 10 Gbps para Switches de Acesso.

Arquitetura de hardware:

- 24 portas SFP28 por equipamento
- Suporte nativo a 1G, 10G e 25G
- Capacidade mínima de comutação por equipamento: 2.000 Gbps
- Capacidade de encaminhamento mínima: 1.488 milhões de pacotes por segundo (Mpps)

Empilhamento (Stacking):

- Empilhamento físico por portas dedicadas de hardware
- Capacidade mínima de empilhamento: 1 Tbps por stack
- Suporte para 8 switches por pilha

Uplink e Downlinks:

- 2 portas QSFP28
- Suporte a 40G e 100G

Alta disponibilidade e Energia:

- Fontes de alimentação redundantes hot-swap
- Ventiladores hot-swap
- Suporte a StackPower
- Operação contínua mesmo em falha de fonte ou ventilador

Funcionalidades de Camada de rede:

- Layer 2 avançado: IEEE 802.1Q (VLAN tagging), MSTP (802.1s) e RSTP Proteções de STP, Link Aggregation (LACP), IGMP Snooping, Storm Control (broadcast, multicast e unicast desconhecido), LLDP e CDP.
- Layer 3: Static Routing, OSPFv2, VRRP / Warm Spare, Multicast PIM-SM, DHCP Server e DHCP Relay.

Segurança

- IEEE 802.1X
- MAB (MAC Authentication Bypass)
- ACL IPv4 e IPv6 em hardware
- DHCP Snooping
- Dynamic ARP Inspection
- Port Security

7.4. **SWITCH ACESSO**

Responsáveis pela conexão direta de dispositivos finais e access points, fornecendo conectividade cabeada multigigabit, alimentação PoE/PoE++ e aplicação inicial de políticas de acesso à rede.

Modelo considerado: Cisco Meraki MS150-48MP-4X

Características mínimas:

- Empilhamento físico entre os switches.
- Uplinks de 10 Gbps (Core ou Distribuição).
- Mínimo de 16 portas multigigabit (mGig 2.5G/5G) por equipamento.
- Suporte a PoE+/PoE++ para alimentação de APs Wi-Fi 7.

Arquitetura de hardware:

- 48 portas RJ-45 por equipamento
- No mínimo 16 portas Multigigabit (2.5G / 5G)
- 4 interfaces SFP+ 10 GbE
- Capacidade mínima de comutação: 304 Gbps

Empilhamento (Stacking):

- Empilhamento físico por portas dedicadas
- Largura de banda de stacking de 80 Gbps

Funcionalidades de Camada de rede:

- Layer 2 avançado: IEEE 802.1Q (VLAN tagging), MSTP (802.1s) e RSTP Proteções de STP, Link Aggregation (LACP), IGMP Snooping, Storm Control (broadcast, multicast e unicast desconhecido), LLDP e CDP.

PoE:

- IEEE 802.3bt (PoE++)
- 60 W por porta multigigabit
- Orçamento mínimo total: 740 W

Segurança:

- IEEE 802.1X
- MAB (MAC Authentication Bypass)
- ACL IPv4 e IPv6 em hardware
- DHCP Snooping
- Dynamic ARP Inspection

7.5. **ACCESS POINT – BAIXA / MÉDIA DENSIDADE**

Responsável por prover conectividade Wi-Fi 7 em ambientes de baixa a média densidade, garantindo cobertura estável, eficiência espectral e desempenho adequado a usuários corporativos e visitantes.

Modelo considerado: Cisco Wireless CW9172I-RTG

Características mínimas:

- Wi-Fi 7 (802.11be).
- Operação tri-band (2.4, 5 e 6 GHz).
- Será posicionado para atender a maioria dos ambientes, de baixa a média densidade de dispositivos conectados simultaneamente.

Padrão e Tecnologia WLAN:

- Padrão IEEE primário: 802.11be (Wi-Fi 7)
- Compatibilidade retroativa: 802.11ax / 802.11ac / 802.11n
- Bandas de operação simultâneas: 2,4 GHz, 5 GHz e 6 GHz

Rádios Integrados:

- Wi-Fi 7 (802.11be) em todos os três rádios
- 2,4 GHz + 5 GHz + 6 GHz (todos 2×2:2) ou 2,4 GHz (2×2:2) + 5 GHz (4×4:4)
- Rádio dedicado para varredura (scan/aux) e rádio IoT (BLE 6)
- Suporte às Tecnologias: DL/UL OFDMA, MU-MIMO, BSS Coloring, Target Wake Time (TWT)

PHY Data Rate agregado:

- Até 9 Gbps (Valor teórico máximo conforme chipset e especificação IEEE 802.11be)

Antenas e ganho:

- Tipo: Antenas internas omnidirecionais
- Ganho por banda:
  - 2,4 GHz: 4 dBi
  - 5 GHz: 5 dBi
  - 6 GHz: 5 dBi

Segurança WLAN:

- WPA2-Enterprise
- WPA3-Enterprise
- WPA3-Personal
- Enhanced Open (OWE)
- 802.1X com:
  - EAP-TLS
  - PEAP
  - EAP-TTLS
- Protected Management Frames (PMF)

Conectividade Ethernet:

- 1 porta Ethernet RJ-45 multigigabit (2,5 Gbps)
- Autonegociação e detecção automática de velocidade.

7.6. **ACCESS POINT - MÉDIA/ ALTA DENSIDADE**

Responsável por prover conectividade Wi-Fi 7 em ambientes de média a alta densidade, suportando alta concentração de dispositivos simultâneos com maior capacidade, throughput e eficiência RF.

Modelo considerado: Cisco Wireless CW9176I-RTG

Características mínimas:

- Wi-Fi 7 de alta capacidade.
- Operação tri-band (2.4, 5 e 6 GHz).
- Será posicionado para atender ambientes específicos, de média a alta densidade de dispositivos conectados simultaneamente.

Padrão e Tecnologia WLAN:

- Padrão IEEE primário: 802.11be (Wi-Fi 7)
- Compatibilidade retroativa: 802.11ax / 802.11ac / 802.11n
- Bandas de operação simultâneas: 2,4 GHz, 5 GHz e 6 GHz

Rádios Integrados:

- Rádio de acesso a clientes 2,4 GHz compatível com 802.11b/g/n/ax/be *(ou)*
- Rádio de acesso a clientes 5 GHz compatível com 802.11a/n/ac/ax/be *(rádio flexível em modo XOR)*
- Rádio de acesso a clientes 5 GHz compatível com 802.11a/n/ac/ax/be
- Rádio de acesso a clientes 6 GHz compatível com 802.11ax/be
- Rádio IoT 2,4 GHz
- Rádio tri-band (2,4 GHz, 5 GHz e 6 GHz) dedicado ao Air Marshal (WIDS/WIPS), análise espectral e analytics de localização
- Rádio Bluetooth Low Energy (BLE) 2,4 GHz com suporte a Beacon e varredura BLE
- Operação simultânea dos cinco rádios.

- BLE versão 5.3, com possibilidade de atualização por software para versão 6.0 no futuro.

PHY Data Rate agregado:

- Até 18 Gbps (Valor teórico máximo conforme chipset e especificação IEEE 802.11be)

Antenas e ganho:

- Tipo: Antenas internas omnidirecionais
- Ganho por banda:
    - 2,4 GHz: 5 dBi
    - 5 GHz: 5 dBi
    - 6 GHz: 6 dBi

Segurança WLAN:

- WPA2-Enterprise
- WPA3-Enterprise
- WPA3-Personal
- Enhanced Open (OWE)
- 802.1X com:
    - EAP-TLS
    - PEAP
    - EAP-TTLS
- Protected Management Frames (PMF)

Conectividade Ethernet:

- 1 porta Ethernet RJ-45 multigigabit (10 Gbps)
- Autonegociação e detecção automática de velocidade.

8. PLATAFORMA DE GESTÃO E AUTOMAÇÃO OPERACIONAL DE REDE

Plataforma de Gerenciamento em Nuvem

8.1. **Descrição da solução**

A Gestão dos ativos de rede deverá ser realizada através do Cisco Meraki Dashboard, plataforma de gestão e automação operacional de rede, baseada em nuvem, responsável pelo provisionamento, configuração, monitoramento e visibilidade da infraestrutura. A plataforma opera exclusivamente no plano de controle, não encaminha tráfego de dados e elimina a necessidade de controladores locais, garantindo alta disponibilidade, automação operacional e simplicidade na gestão da rede.

8.2. **Arquitetura da Plataforma**

A solução de gerenciamento deverá operar com separação lógica e funcional entre:

- **Plano de Controle (Control Plane)**: executado na nuvem do Meraki Dashboard;
- **Plano de Dados (Data Plane)**: executado localmente nos switches e access points.

O tráfego de dados da rede local não deverá, em nenhuma hipótese, transitar pela nuvem, sendo restrita à nuvem apenas a troca de informações de gerenciamento, eventos, estatísticas e comandos administrativos.

A comunicação entre os equipamentos de rede e a plataforma deverá obedecer aos seguintes requisitos:

a. Comunicação iniciada exclusivamente pelos equipamentos (outbound);
b. Utilização de conexões seguras baseadas em HTTPS/TLS;
c. Inexistência de necessidade de portas de entrada (inbound) abertas na rede da Contratante;
d. Não exigência de túneis VPN site-to-cloud;

8.3. **Disponibilidade e Resiliência Operacional**

A indisponibilidade temporária da conectividade com a nuvem não deverá interromper o funcionamento da rede local, devendo os equipamentos:

a. Continuar operando com a última configuração válida;
b. Manter políticas de VLAN, segurança, QoS e RF ativas;
c. Permitir o encaminhamento normal do tráfego de dados dos usuários.

A plataforma deverá operar em ambiente de nuvem distribuído, com:

a. Datacenters redundantes;
b. Mecanismos automáticos de failover;
c. Alta disponibilidade do serviço de gerenciamento;
d. Manutenção e atualização da plataforma sob responsabilidade do fabricante.

8.4. **Funcionalidades da Plataforma de Gestão e Automação Operacional de rede**

A plataforma de gerenciamento deverá suportar, no mínimo, as seguintes funcionalidades:

- Provisionamento centralizado (Zero-Touch Provisioning) dos equipamentos;
- Configuração remota de:
    - VLANs;
    - portas de acesso e uplink;

  - SSIDs e políticas wireless;
  - perfis de RF;
  - QoS;
- Monitoramento em tempo real de:
  - estado dos equipamentos;
  - portas e interfaces;
  - clientes conectados;
  - aplicações identificadas;
- Geração de alertas operacionais;
- Atualizações centralizadas de firmware;
- Registro de eventos operacionais;
- Disponibilização de **APIs REST** para automação e integração.

8.5. **Dados coletados, Visibilidade e retenção**

A plataforma deverá disponibilizar dados operacionais, incluindo, no mínimo:

a. Estado e saúde dos equipamentos;
b. Eventos de porta (up/down);
c. Estatísticas de throughput;
d. Informações de clientes (endereço MAC, IP, SSID);
e. Eventos de associação e roaming wireless;
f. Identificação de aplicações.

A retenção dos dados deverá seguir as políticas do fabricante, sendo disponibilizados:

a. Dados históricos agregados;
b. Exportação de informações por meio de interface gráfica ou APIs;

8.6. **Segurança e Controle Administrativo**

A solução de gerenciamento deverá atender aos seguintes requisitos de segurança:

a. Comunicação criptografada entre equipamentos e nuvem;

b. Autenticação segura baseada em certificados;
c. Controle de acesso administrativo baseado em perfis;
d. Registro de ações administrativas realizadas na plataforma.

8.7. **Licenciamento da Plataforma**

O licenciamento da plataforma de gerenciamento em nuvem deverá observar:

a. Licenciamento obrigatório para operação contínua dos equipamentos;
b. Vigência mínima de licenciamento conforme definido neste Termo de Referência;
c. Manutenção da solução em estado de conformidade durante todo o período contratual.

8.8. **Integrações Suportadas**

A plataforma deverá suportar integração nativa ou via APIs com:

a. Cisco Spaces;
b. Cisco ISE;
c. Soluções externas de monitoramento e automação;

9. SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC)

Cisco Identity Services Engine

9.1. **Descrição Geral da Solução**

A solução de Controle de Acesso à Rede (NAC) deverá ser baseada na plataforma Cisco Identity Services Engine (ISE).

O Cisco Identity Services Engine (Cisco ISE) é uma plataforma de Controle de Acesso à Rede (NAC) responsável pela autenticação, autorização e contabilização (AAA) de usuários e dispositivos na rede corporativa, com base em identidade.

A plataforma atua de forma centralizada e fora do plano de dados, utilizando decisões de acesso baseadas em atributos RADIUS clássicos, sem interferir no encaminhamento do tráfego da rede.

9.2. **Enquadramento da Plataforma no escopo**

Embora o Cisco ISE possua funcionalidades avançadas para diversos cenários de segurança e segmentação, serão exigidas exclusivamente as funcionalidades compatíveis com:

- Licenciamento Cisco ISE Essentials;
- Arquitetura Small Deployment;

Neste contexto, o Cisco ISE não será utilizado como plataforma de segmentação avançada, automação baseada em intenção ou resposta a ameaças, limitando-se ao escopo funcional definido neste capítulo.

9.3. **Arquitetura da Solução**

A solução deverá ser implantada minimamente no modelo “Small Deployment”, respeitando integralmente os limites de capacidade, desempenho e escalabilidade associados a este porte.

A solução deverá suportar, no mínimo:

- 25.000 (vinte e cinco mil) sessões simultâneas ativas.

A solução deverá suportar implementar, no mínimo, todas as personas do ISE (PAN, MnT, PSN e pxGrid) no mesmo appliance ou instâncias de máquina virtual.

- Policy Administration Node (PAN): Responsável pela administração centralizada, definição e distribuição de políticas, interface gráfica e APIs.
- Policy Service Node (PSN): Responsável pela autenticação e autorização de acessos (IEEE 802.1X e MAB), bem como accounting RADIUS.
- Monitoring and Troubleshooting Node (MnT): Responsável pela coleta de logs, relatórios, auditoria e troubleshooting.
- pxGrid Node: Responsável pela integração com plataformas externas, incluindo Cisco Meraki Dashboard, Cisco Spaces e sistemas de SIEM.

A solução de Controle de Acesso à Rede (NAC) deverá ser implantada conforme as seguintes diretrizes:

a) Implantação 100% virtualizada, em ambiente de virtualização disponibilizado pela Contratante;
b) Arquitetura Small Deployment, contemplando os serviços PAN, PSN e MnT, conforme boas práticas do fabricante;

c) Dimensionamento das máquinas virtuais equivalente ao appliance físico Cisco SNS 3815, incluindo CPU, memória e armazenamento, cabendo à Contratante a responsabilidade pela disponibilização, alocação e garantia dos recursos de infraestrutura necessários ao correto funcionamento da solução;
d) A Contratada será responsável exclusivamente pela instalação, configuração lógica e validação da plataforma, não sendo responsável pelo fornecimento de hardware, hypervisor ou capacidade computacional do ambiente virtualizado;
e) A alta disponibilidade da solução deverá ser garantida por meio da arquitetura lógica definida, considerando que os recursos de virtualização subjacentes são de responsabilidade da Contratante.

A solução deverá suportar arquitetura de alta disponibilidade, contemplando:

- Implementação em dois nós, sendo:
  - um nó configurado como primário;
  - um nó configurado como secundário, para fins de redundância.
- Failover automático do PAN;
- Continuidade operacional dos PSNs.

A solução de NAC será aplicada exclusivamente à rede corporativa, sendo obrigatória a garantia de que:

- O Cisco ISE não seja utilizado para autenticação da rede Visitante;
- Não tratativa das sessões da rede Visitante;
- O acesso Visitante seja tratado exclusivamente pela solução especificada responsável pelo Portal Cativo.

No contexto deste projeto, a solução de NAC deverá fornecer, no mínimo, as seguintes funcionalidades para a rede corporativa:

a) Autenticação baseada em identidade

- IEEE 802.1X para usuários e dispositivos;
- MAB (MAC Authentication Bypass) para dispositivos que não suportem IEEE 802.1X;
- Integração com fontes de identidade (ex.: Active Directory), quando requerido.

b) Autorização baseada em identidade (AAA clássico)

Após a autenticação, o Cisco ISE deverá aplicar autorização baseada em identidade, por meio da utilização de perfis de autorização (Authorization Profiles) baseados em atributos RADIUS, permitindo definir o que o usuário ou dispositivo pode ou não acessar.

Essa autorização poderá incluir, conforme aplicável:

- Associação dinâmica a VLANs (se aplicável);
- Aplicação de políticas básicas de acesso por meio de atributos RADIUS;
- Definição de parâmetros de sessão (ex.: timeout).

Não serão utilizados mecanismos de segmentação avançada, tais como TrustSec, SGT, Segmentação baseada em rótulos, Políticas baseadas em contexto avançado, ou SD-Access.

c) Contabilização e visibilidade

- Registro de eventos de autenticação e autorização;
- Registro de data, hora, identidade autenticada e método de acesso;
- Consulta e exportação de logs para auditoria técnica.

d) Integração com a infraestrutura de rede

- Integração nativa com a infraestrutura de rede e plataforma de gerenciamento para aplicação das decisões AAA;
- Operação compatível com rede cabeada e sem fio;

Para fins de delimitação contratual, não são exigidas neste Termo de Referência, ainda que tecnicamente suportadas pela plataforma Cisco ISE:

a. Funcionalidades associadas aos licenciamentos Advantage ou Premier;
b. TrustSec, Security Group Tags (SGT) ou segmentação baseada em rótulos;
c. SD-Access ou automação baseada em intenção;
d. Avaliação de postura de endpoints (Posture);
e. Detecção ou resposta a ameaças;
f. Uso do Cisco ISE para autenticação ou controle da rede Visitante.

A ausência dessas funcionalidades não caracterizará não conformidade, desde que o escopo funcional exigido seja plenamente atendido.

A solução de Controle de Acesso à Rede deverá operar de forma integrada à Plataforma de Gestão e Automação Operacional de Rede, de modo a fornecer visibilidade operacional das autenticações e sessões de acesso, sem que haja transferência ou sobreposição de funções entre as plataformas.

A integração entre o Cisco Identity Services Engine e a Meraki Dashboard terá como finalidade:

- Exibir informações operacionais sobre clientes autenticados;
- Correlacionar identidade, método de autenticação, porta ou ponto de acesso;
- Apoiar atividades de operação e troubleshooting da rede.

A solução deverá permitir:

- Registro e consulta de eventos de autenticação e autorização;
- Exportação de logs para auditoria técnica;
- Suporte a processos de auditoria e fiscalização;
- Operação conforme boas práticas de segurança do fabricante.

10. PLATAFORMA DE INTELIGÊNCIA, ANALYTICS E EXPERIÊNCIA PARA REDE WIRELESS

A solução deverá ser baseada no Cisco Spaces, uma plataforma em nuvem da Cisco destinada à coleta, processamento e análise de dados contextuais da rede sem fio, utilizando telemetria proveniente dos access points para fornecer serviços de analytics, visibilidade, experiências digitais e integração com aplicações de negócio.

A solução opera de forma independente do plano de dados, utilizando apenas informações de controle e eventos de associação dos dispositivos à rede Wi-Fi, não realizando inspeção de conteúdo de tráfego.

Embora o Cisco Spaces possua capacidades adicionais para múltiplos casos de uso, serão exigidas exclusivamente as funcionalidades relacionadas ao controle e gestão para a rede visitantes.

Neste contexto, o Cisco Spaces não será adotado como plataforma de analytics corporativo avançado, localização de alta precisão ou engajamento digital, limitando-se ao escopo funcional definido neste capítulo.

No contexto deste projeto, o Cisco Spaces deverá fornecer, no mínimo, as seguintes funcionalidades para a Rede Visitante:

- Portal Cativo (Captive Portal) para onboarding de usuários visitantes, com suporte a:
    - Aceite de termos de uso;

    - Autenticação baseada em formulário (ex.: nome, e-mail, telefone ou outro dado definido pela Contratante);
    - Customização visual do portal, incluindo identidade visual e textos legais;
    - Entrega de experiências condicionais, baseadas em regras e contexto (ex.: visitante novo ou recorrente);
    - Reconhecimento de visitantes recorrentes, conforme capacidades do Cisco Spaces e limitações do licenciamento;
    - Redirecionamento pós-autenticação para URL definida pela Contratante;
- Registro de eventos de associação e sessão, incluindo:
    - endereço MAC do dispositivo;
    - SSID utilizado;
    - ponto de acesso associado;
    - data e hora de início e término da sessão;
- Analytics básicos de usuários visitantes, tais como:
    - número de visitantes;
    - sessões ativas e históricas;
    - tempo de permanência;
- Visibilidade operacional da rede visitante, permitindo consulta e exportação de informações;
- Integração com a Plataforma de Gestão e Automação Operacional de Rede, para fins de configuração, telemetria e operação.

Para fins de delimitação de escopo contratual, não são exigidas neste Termo de Referência, ainda que tecnicamente suportadas pela plataforma Cisco Spaces:

- Casos de uso avançados de localização em tempo real (RTLS);
- Analytics avançados de comportamento ou fluxo de pessoas;

- Funcionalidades de engajamento digital, campanhas ou marketing;
- Integrações com aplicações de negócio ou sistemas externos além do escopo visitante;

A ausência dessas funcionalidades não caracterizará não conformidade, desde que o escopo funcional definido neste capítulo seja plenamente atendido.

A plataforma Cisco Spaces deverá operar integrada à infraestrutura wireless e à Plataforma de Gestão e Automação Operacional de Rede, respeitando os seguintes princípios:

- Integração nativa com a infraestrutura Wi-Fi;
- Consumo apenas de dados de controle e eventos de associação;
- Ausência de dependência de controladores ou servidores locais;
- Operação independente da solução de Controle de Acesso à Rede (NAC).

O Cisco Spaces não deverá substituir nem interferir nas funções de autenticação e autorização da rede corporativa.

A solução deverá permitir o atendimento aos requisitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados (LGPD), assegurando que:

- Apenas dados estritamente necessários ao controle de acesso Visitante sejam coletados;
- Não haja inspeção de conteúdo de tráfego;
- Os registros de conexão possam ser consultados e exportados, com prazo mínimo de 1 (um) ano;
- Os dados sejam protegidos contra acesso não autorizado.

A solução deverá permitir:

- Exportação de dados para fins de auditoria técnica ou legal;
- Consulta histórica de eventos;
- Controle de acesso administrativo baseado em perfis.

A solução deverá garantir:

- Comunicação criptografada entre componentes;
- Proteção contra reutilização ou sequestro de sessões;
- Operação conforme as boas práticas definidas nos runbooks Cisco Spaces.

11. LICENCIAMENTO, GARANTIA E SUPORTE

- Todos os componentes da solução deverão ser fornecidos com licenciamento válido para 5 (cinco) anos.
- Garantia oficial do fabricante e direito a atualizações de softwares durante todo o período.

12. SERVIÇOS PROFISSIONAIS - IMPLEMENTAÇÃO

12.1. Objetivo dos Serviços Profissionais

A Contratada deverá executar serviços profissionais especializados para implementação da solução descrita neste Termo de Referência, contemplando planejamento técnico, implantação, integração, testes, validação e documentação, assegurando que todos os componentes da arquitetura estejam operacionais, aderentes às premissas técnicas e alinhados às boas práticas do fabricante.

Os serviços deverão ser executados por profissionais qualificados e certificados, com experiência comprovada em projetos de infraestrutura de rede corporativa de porte e complexidade compatíveis com o escopo deste projeto.

12.2. Camada de Core

A Contratada deverá executar todas as atividades necessárias para a implantação da camada de Core, assegurando alta disponibilidade, desempenho e convergência da rede. As atividades incluem, no mínimo:

- Planejamento físico e lógico (HLD/LLD) da camada de Core, considerando topologia, empilhamento, redundância de enlaces e integração com as demais camadas;
- Implantação lógica dos switches de Core, incluindo empilhamento, fontes redundantes e módulos de uplink;
- Integração dos switches de Core à Plataforma de Gestão e Automação Operacional de Rede;
- Configuração de interfaces de uplink e downlink, respeitando velocidades, agregações e arquitetura definida;
- Implementação de protocolos de camada 2 e camada 3 conforme planejamento lógico, garantindo estabilidade e convergência adequada;
- Configuração de mecanismos de resiliência, controle de loops e proteção da topologia;
- Validação funcional da camada, incluindo testes de redundância, failover e conectividade com Distribuição, ToR e Acesso.

12.3. Camada de Distribuição

A Contratada deverá implantar a camada de Distribuição como elemento de agregação e interligação entre Core e Acesso, executando, no mínimo, as seguintes atividades:

- Planejamento físico e lógico (HLD/LLD) por área atendida, considerando empilhamento em pares, uplinks redundantes e segmentação definida;
- Implantação lógica dos switches de Distribuição;
- Integração dos switches à Plataforma de Gestão e Automação Operacional de Rede;
- Configuração de empilhamento, uplinks com a camada de Core e downlinks com a camada de Acesso;
- Implementação de protocolos de camada 2 e camada 3 conforme planejamento lógico, garantindo estabilidade e convergência adequada;
- Configuração de mecanismos de resiliência, controle de loops e proteção da topologia;
- Testes de conectividade, desempenho e resiliência entre Distribuição, Core e Acesso.

12.4. **Camada de topo de rack (ToR)**

- A Contratada deverá implantar a camada de Topo de Rack destinada à agregação de servidores e infraestrutura, executando, no mínimo:
- Planejamento físico e lógicos (HLD/LLD) da interligação dos switches ToR com a camada de Core;
- Implantação e lógica dos switches ToR, incluindo empilhamento e redundância;
- Configuração de uplinks de alta capacidade e baixa latência;
- Configuração de portas de acesso para servidores e equipamentos de infraestrutura;
- Implementação de protocolos de camada 2 e camada 3 conforme planejamento lógico, garantindo estabilidade e convergência adequada;
- Configuração de mecanismos de resiliência, controle de loops e proteção da topologia;
- Integração dos switches ToR à Plataforma de Gestão e Automação Operacional de Rede;
- Validação da conectividade e desempenho dos enlaces ToR–Core e ToR–servidores.

12.5. **Camada de Acesso**

A Contratada deverá executar a implantação completa da camada de Acesso, responsável pela conexão de dispositivos finais e access points, incluindo:

- Planejamento físico e lógico (HLD/LLD) das portas de acesso e uplinks;
- Implantação lógica dos switches de Acesso;
- Integração dos switches de Acesso à Plataforma de Gestão e Automação Operacional de Rede;

- Configuração de portas de acesso para dispositivos finais e access points, incluindo parâmetros de PoE/PoE++;
- Configuração dos uplinks para Core ou Distribuição conforme arquitetura definida;
- Testes de conectividade com dispositivos finais, access points e camadas superiores;
- Validação da segregação lógica entre rede corporativa e rede de visitantes.

12.6. **Camada de Wireless**

A Contratada deverá executar a implantação da camada Wireless, assegurando cobertura, capacidade e qualidade de serviço, incluindo:

- Planejamento físico e lógico da implantação dos access points conforme site survey preditivo realizado previamente;
- Integração dos access points à Plataforma de Gestão e Automação Operacional de Rede;
- Configuração de SSIDs, parâmetros de segurança e políticas operacionais;
- Configuração de parâmetros RF, incluindo canais, potências e bandas;
- Garantia de segregação lógica entre rede corporativa e rede de visitantes;
- Validação funcional da conectividade wireless.

12.7. **Plataforma de Gestão e Automação Operacional de Rede**

Os serviços de Implementação da Plataforma de Gestão e Automação Operacional de Rede deverão contemplar, no mínimo:

- Integração de todos os switches e Access Points;
- Organização lógica dos equipamentos (sites, redes, grupos);
- Configuração de perfis de administração e controle de acesso;
- Ativação de monitoramento e alertas;
- Validação de visibilidade por:
    - equipamento;
    - porta;
    - cliente;
    - aplicação.
- Integração à plataforma de inteligência, analytics e experiência sobre a rede wireless;

12.8. **Controle de Acesso à Rede (NAC)**

A Contratada deverá executar as atividades necessárias para a implantação da solução de NAC, incluindo:

- Instalação da solução em ambiente virtualizado disponibilizado pela Contratante;
- Configuração da arquitetura Small Deployment conforme boas práticas do fabricante;
- Implementação de autenticação baseada em identidade (802.1X e MAB);
- Configuração de autorização baseada em identidade por meio de AAA clássico;
- Integração do NAC com a infraestrutura cabeada e wireless;
- Validação das autenticações, autorizações e registros de eventos;
- Garantia de aplicação exclusiva à rede corporativa.

12.9. **Plataforma de Inteligência, Analytics e Experiência sobre a Rede Wireless**

A Contratada deverá executar as seguintes atividades relacionadas à plataforma de analytics wireless:

- Integração da infraestrutura wireless à plataforma;
- Configuração das funcionalidades aplicáveis ao ambiente de visitantes, conforme escopo definido no TR;
- Habilitação da coleta e correlação de eventos de associação e sessão;
- Validação da visibilidade operacional e rastreabilidade das conexões;
- Garantia de que funcionalidades fora do escopo não sejam habilitadas.

12.10. **Integração entre Plataformas**

A Contratada deverá garantir a correta integração operacional entre:

- Infraestrutura de rede;
- Plataforma de Gestão e Automação Operacional de Rede;
- Solução de Controle de Acesso à Rede (NAC);
- Plataforma de inteligência, analytics e experiência sobre a rede wireless.

As integrações deverão respeitar os limites funcionais de cada solução, sem sobreposição de papéis, conforme definido neste Termo de Referência.

12.11. **Site Survey Ativo de Rede Wireless**

A Contratada deverá executar Wireless Site Survey Ativo pós-implantação, com a rede wireless em plena operação, contemplando:

- Validação de cobertura, qualidade RF e desempenho
- Coleta de métricas reais de sinal, SNR, taxa de associação e roaming;
- Identificação de eventuais áreas de não conformidade;
- Elaboração de relatório técnico detalhado.

Eventuais ajustes identificados deverão ser realizados pela Contratada, seguidos de nova validação.

12.12. **Testes, Validação e Aceite Técnico**

A Contratada deverá executar testes funcionais e operacionais, incluindo:

- Testes de conectividade por camada;
- Testes de autenticação e autorização da rede corporativa;
- Testes de acesso e visibilidade da rede de visitantes;
- Validação da segregação lógica entre os domínios;
- Validação de visibilidade e automação operacional.

A solução somente será considerada implementada após aprovação formal da Contratante.

12.13. **Documentação técnica**

A Contratada deverá entregar documentação técnica completa, incluindo, no mínimo:

- Arquitetura física e lógica final da solução (HLD e LLD);
- Configurações aplicadas;
- Diagramas atualizados;
- Relatório do Wireless Site Survey Ativo;
- Procedimentos básicos de operação.

12.14. **Limites de Responsabilidade**

Caberá à Contratada a implantação lógica, configuração, integração e validação da solução.

Caberá à Contratante a disponibilização de infraestrutura física e de virtualização, incluindo recursos computacionais necessários às soluções implantadas.

Thiago de Lima Barbosa
Thiago de Lima Barbosa (20/03/2026 16:32:24 ADT)

Thiago de Lima Barbosa

Coordenador de Infraestrutura de T.I.

Augusto Berti
Augusto Berti (20/03/2026 16:33:35 ADT)

Augusto Berti Neto

Coordenador de Sistemas

ANEXO I - ESPECIFICAÇÃO TÉCNICA - HARDWARE DE REDE

Relatório de auditoria final 2026-03-20

Criado em:	2026-03-20 (Horário Padrão de Brasília)
Por:	Thiago de Lima Barbosa (thiago.barbosa@itamed.com.br)
Status:	Assinado
ID da transação:	CBJCHBCAABAAqvvhoZAMo4zNbDfzPMVlHAxyHQ7_Z-xi

Histórico de "ANEXO I - ESPECIFICAÇÃO TÉCNICA - HARDWARE DE REDE"

Documento criado por Thiago de Lima Barbosa (thiago.barbosa@itamed.com.br)
2026-03-20 - 16:30:39 ADT

Documento enviado por email para Thiago de Lima Barbosa (thiago.barbosa@itamed.com.br) para assinatura
2026-03-20 - 16:32:00 ADT

Documento assinado eletronicamente por Thiago de Lima Barbosa (thiago.barbosa@itamed.com.br)
Data da assinatura: 2026-03-20 - 16:32:24 ADT - Fonte da hora: servidor

Documento enviado por email para Augusto Berti (augusto.berti@itamed.com.br) para assinatura
2026-03-20 - 16:32:25 ADT

Email visualizado por Augusto Berti (augusto.berti@itamed.com.br)
2026-03-20 - 16:32:37 ADT

Documento assinado eletronicamente por Augusto Berti (augusto.berti@itamed.com.br)
Data da assinatura: 2026-03-20 - 16:33:35 ADT - Fonte da hora: servidor

Contrato finalizado.
2026-03-20 - 16:33:35 ADT