ANEXO I - ESPECIFICAÇÕES TÉCNICAS

Item	Descrição	Catálogo	Unidade de Medida	Quantidade
1	Switch de Núcleo	CATMAT 393273	Unidade	4
2	Switch de Acesso	CATMAT 393274	Unidade	50
3	Ponto de acesso sem fio - Indoor	CATMAT 404260	Unidade	125
4	Transceiver SFP+ 10G	CATMAT 618351	Unidade	100
5	Solução de Gerenciamento	CATSER 27014	Unidade	1
6	Plataforma de Controle de Acesso à Rede (NAC)	CATSER 27022	Unidade	1

0.1. A Solução de Conectividade de Rede Local (LAN) e Wireless (WLAN) compreende a aquisição de switches de núcleo, switches de acesso, pontos de acesso de rede sem fio, softwares de gerenciamento e licenciamento, abrangendo o fornecimento de todos os equipamentos, acessórios, peças e componentes necessários à sua completa implantação e operação no MCID;

0.2. A contratação inclui, de forma integrada, a prestação de serviços de instalação física, configuração lógica e suporte técnico especializado com garantia de funcionamento em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), pelo período mínimo de 60 (sessenta) meses;

0.3. Para fins de interpretação das exigências contidas neste documento, aplicam-se as seguintes definições:

0.3.1. Suportar / Permitir: Significa que o equipamento deve possuir a capacidade técnica e arquitetural para a função, mesmo que dependa de licenciamento ou hardware adicional futuro para ativação de novos recursos; e

0.3.2. Possuir / Fornecer / Implementar: Significa que a funcionalidade deve estar disponível para uso imediato, com todas as licenças, cabos e componentes inclusos no valor da proposta, sem custos adicionais ao Ministério.

0.4. REQUISITOS DE IMPLEMENTAÇÃO E INSTALAÇÃO

0.5. A CONTRATADA deverá realizar a implantação integral da solução, compreendendo o planejamento físico e lógico, a montagem dos ativos nos racks e a instalação física de todos os itens de hardware;

0.6. Os serviços abrangem a passagem, organização e conexão de todo o cabeamento necessário (Ethernet e/ou fibra óptica), bem como a configuração das políticas de segurança, segmentação de rede e a transferência de conhecimento para a equipe técnica do CONTRATANTE;

0.7. INTEGRIDADE E PADRONIZAÇÃO DA SOLUÇÃO

0.8. Para fins de garantia da interoperabilidade plena, performance da gerência unificada e suporte técnico centralizado, todos os switches (núcleo e acesso), pontos de acesso de rede sem fio, solução de gerenciamento e plataforma de controle e acesso à rede (NAC) deverão obrigatoriamente ser do mesmo fabricante;

0.9. A exigência de fabricante único visa assegurar a integração nativa dos recursos de segurança, automação via Zero Touch Provisioning (ZTP), telemetria avançada e a orquestração centralizada de políticas de acesso em toda a infraestrutura de rede do MCID;

0.10. Todos os componentes fornecidos deverão pertencer a linhas de produtos que guardem total compatibilidade entre si, sendo entregues em suas versões mais recentes, em linha de produção ativa e sem previsão de descontinuidade (end-of-life) pelo fabricante durante o período de suporte contratado;

0.11. A solução será entregue com todas as licenças e recursos funcionais habilitados para uso imediato, com subscrições válidas por 60 meses, assegurando ao MCID o direito de uso e atualização das ferramentas de gestão durante todo o ciclo de vida contratual;

0.12. CONDIÇÕES PARA COMPROVAÇÃO TÉCNICA

0.13. A licitante deverá detalhar em sua proposta cada componente ofertado, indicando obrigatoriamente marca, modelo e part number, para garantir total clareza sobre os produtos e serviços;

0.14. A conformidade com os requisitos técnicos deverá ser demonstrada mediante a apresentação

de manuais ou catálogos oficiais do fabricante. Declarações da licitante ou de distribuidores não serão aceitas como substitutas da documentação oficial;

0.15. Caberá à licitante apresentar provas formais de atendimento às especificações, indicando na documentação pública do fabricante (em formato impresso ou eletrônico) a página ou seção exata em que cada requisito é contemplado, de modo a permitir a verificação inequívoca pela equipe técnica do Ministério;

1. ITEM 1 - SWITCH DE NÚCLEO

1.1. Deve possuir no mínimo 48 (quarenta e oito) portas frontais de comunicação nativas de SFP+ (1/10 Gbps) ou SFP28 (25 Gbps). No caso de oferta de portas SFP28, estas deverão obrigatoriamente suportar a operação em velocidades de 1 Gbps e 10 Gbps (SFP+). Adicionalmente, deve possuir no mínimo 6 (seis) portas frontais para uplinks e empilhamento, com velocidade mínima de 40 Gbps cada (aceitando-se tecnologias de 40 Gbps, 100 Gbps ou superiores), utilizando slots do tipo QSFP+ ou QSFP28;

1.2. Deve possuir capacidade de comutação total mínima (switching) de 2,1 Tbps;

1.3. Deve possuir capacidade para encaminhamento de pacotes de no mínimo 480 (quatrocentos e oitenta) Mpps;

1.4. Deve permitir instalação em rack de 19” padrão Telco EIA, incluindo todos os acessórios para fixação, devendo ocupar no máximo 1 (um) rack unit (RU);

1.5. Deve possuir fonte de alimentação interna com ajuste automático de tensão entre 110 e 220V AC, e frequência 50/60 Hz;

1.6. Deve possuir no mínimo 2 (duas) fontes de alimentação internas, redundantes, de mesma capacidade e hot-swappable, de forma que no caso da falha de uma das fontes as demais tenham capacidade para alimentar o switch em sua capacidade total;

1.7. Deverão ser fornecidos cabos de alimentação para todas as fontes do switch no padrão NBR 14136;

1.8. Possuir módulos de ventilação (Fan Trail) redundantes, com fluxo de ar “Front-to-Back”, internas, Hot-Swap, independentes entre si. Todos os slots de Fan devem estar ocupados;

1.9. Deverá suportar o uso dos transceivers adquiridos nessa solução;

1.10. Deverá ser fornecido, para cada unidade de switch, 01 (um) conjunto individual e completo de acessórios destinados à interconexão em cluster/empilhamento incluindo módulos, transceivers e cabos). O fornecimento deve ser realizado na proporção de um kit para cada equipamento, garantindo que cada unidade possua seus próprios meios de conexão de forma independente;

1.11. Os meios de interconexão referidos no item anterior devem possuir capacidade de transmissão mínima de 40 Gbps por link (sendo aceitas tecnologias superiores, como 100 Gbps) e comprimento mínimo de 1 (um) metro. Serão aceitas soluções via cabos do tipo AOC, DAC ou através de interfaces ópticas (transceivers) com seus respectivos cordões de fibra compatíveis;

1.12. Os switches devem operar com velocidades diferentes em quaisquer interfaces, sem restrições de grupos de portas operarem em uma mesma velocidade;

1.13. Deve permitir empilhamento físico ou virtual (cluster) e permitir gerenciar a pilha com um único endereço IP;

1.13. Deve permitir empilhamento físico ou virtual (cluster), permitindo o gerenciamento da pilha ou cluster como uma única entidade lógica por meio de endereço IP único ou interface de gerência centralizada;

1.14. Deve suportar a adição ou retirada de switches na pilha ou cluster sem a interrupção dos outros equipamentos;

1.15. As configurações alteradas deverão ser automaticamente replicadas para todos os membros da pilha ou cluster;

1.16. Deve possuir LEDs indicadores de status de funcionamento, fonte de alimentação, status das portas e indicação de qual switch é o mestre (master) da pilha ou cluster;

1.17. Deve possuir capacidade para armazenar, no mínimo, 2 (duas) imagens distintas do software na memória do equipamento, além de registros de crash (dump) e logs locais;

1.18. O proponente deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado;

1.19. Deve ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de “End of Life” emitidos pelo fabricante;

1.20. Deve possuir certificado de homologação junto à ANATEL;

1.21. Possuir tamanho mínimo da tabela MAC de, no mínimo, 64.000 (sessenta e quatro mil) entradas;

1.22. Implementar tabela ARP para, no mínimo, 32.000 entradas IPv4 e 32.000 entradas IPv6;

1.23. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o protocolo IEEE 802.3ad e IEEE 802.1AX-2008;

1.24. Na criação de grupos de links agregados com portas de diferentes membros da pilha ou cluster de alta disponibilidade, deverá suportar a criação de, no mínimo, 24 grupos por pilha ou cluster;

1.25. Deve permitir a criação de grupos de agregação de links (Link Aggregation) distribuídos entre, no mínimo, 02 (dois) equipamentos distintos pertencentes à mesma pilha ou cluster de alta disponibilidade, garantindo a redundância e o encaminhamento de tráfego mesmo em caso de falha de um dos switches de núcleo;

1.26. Deverá suportar a criação de pelo menos 4.000 VLANs, conforme padrão 802.1Q, sendo pelo menos 1.000 VLANs ativas simultâneas;

1.27. Deve implementar os protocolos Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w) e MSTP (Multiple Spanning Tree Protocol);

1.28. Deve implementar Rapid Per-VLAN spanning tree (RPVST+), ou Per-VLAN spanning tree (PVST+), ou VBST (VLAN-Based Spanning Tree), ou protocolo similar em funcionalidade;

1.29. Deve permitir a criação de VLAN específica para voz (voice VLAN) com associação automática;

1.30. Deve suportar Jumbo frames de no mínimo 9018 Bytes;

1.31. Deve implementar o mecanismo IGMP v1/v2/v3 e IGMP snooping/proxy;

1.32. Deve implementar PIM-SM ou PIM-SSM;

1.33. Deve possuir controle de broadcast, unicast desconhecido e multicast por porta;

1.34. O suporte ao protocolo IPv6 poderá ser evidenciado através da certificação IPv6 Ready Logo ou conformidade com as RFCs: RFC4291, RFC 6724, RFC4443, RFC8200, RFC4862 e RFC4541;

1.35. Deverá permitir a configuração de interfaces virtuais (VLAN Interfaces) para roteamento entre VLANs;

1.36. Deverá implementar o encaminhamento de requisições DHCP (DHCP relay);

1.37. Deve implementar Q-in-Q ou VXLAN;

1.38. Deve implementar o roteamento estático e dinâmico em IPv4/IPv6, BGP/BGP4+ e OSPF/OSPFv3;

1.39. Deve implementar VRRP, com suporte para IPv4 e IPv6, permitindo a configuração de, no mínimo, 60 grupos;

1.40. Implementar listas de controle de acesso (ACL) com capacidade de configuração de no mínimo 1.000 ACLs, com processamento em hardware;

1.41. Capacidade de aplicar ACLs para tráfego de entrada e saída em portas de comunicação ou em interfaces de roteamento de VLANs;

1.42. Filtragem de tráfego baseada em: Endereço MAC de origem/destino, Endereço IP de origem/destino, Portas TCP/UDP e tipo de protocolo;

1.43. Deve implementar controle de acesso por porta usando o padrão IEEE 802.1x, com suporte a autenticação via EAP-PEAP, EAP-TLS e EAP-TTLS;

1.44. Deve implementar associação automática de VLAN e aplicação de ACLs ou roles (papéis) na porta através do download do servidor RADIUS/NAC (Change of Authorization - CoA RFC 5176);

1.45. Implementar controle de acesso para gerenciamento compatível com autenticação TACACS+ e RADIUS;

1.46. Suportar proteção contra ataques “ARP Poisoning”, ARP spoof, DHCP spoof e IP spoof;

1.47. Deve implementar proteção por BPDU (root ou loop);

1.48. Proteção da CPU do switch contra-ataques de negação de Bserviço (DoS);

1.49. Dar shutdown em uma porta sob broadcast storm;

1.50. Suportar o monitoramento e gerenciamento por meio do protocolo SNMP v1, v2c e v3;

1.51. Deverá permitir o acesso de no mínimo 5 sessões simultâneas para gerenciamento remoto através do protocolo SSH v2;

1.52. Deve permitir o gerenciamento local através de porta console (RJ-45, USB ou similar);

1.53. Deverá implementar a RFC 5424 para envio de mensagens de log (syslog);

1.54. Deve suportar a sincronização autenticada do relógio interno através do protocolo NTP ou SNTP;

1.55. Deve permitir o monitoramento de tráfego através dos protocolos NetFlow ou IPFIX (RFC 3917) ou NetStream ou SFLOW;

1.56. Permitir o espelhamento de tráfego (Port Mirror) de entrada, saída ou ambos, para porta local ou remota (RSPAN);

1.57. Deverá implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) em nível 2 (IEEE 802.1ag) e nível 3 (ICMP Echo, UDP Jitter);

1.58. Deve implementar 8 (oito) filas de prioridade por porta, permitindo a atribuição de pesos distintos para cada fila;

1.59. Deve executar o processamento do QoS em hardware (Strict Priority e WRR/DRR);

1.60. Classificação baseada em: Porta, IP origem/destino, Portas TCP/UDP, MAC, prioridade 802.1p ou DSCP;

1.61. Permitir o mapeamento e a remarcação de prioridades (802.1p para DSCP e vice-versa);

1.62. Permitir a aplicação de traffic-shaping e rate-limiting;

1.63. Deve suportar a ativação futura de Telemetria, VXLAN e BGP EVPN;

2. ITEM 2 - SWITCH DE ACESSO

2.1. Deve possuir no mínimo 48 (quarenta e oito) portas Ethernet 10/100/1000Base-T com conectores RJ45 e suporte a Power over Ethernet (PoE e PoE+) conforme padrões IEEE 802.3af e IEEE 802.3at;

2.2. Deve possuir no mínimo 4 (quatro) portas nativas SFP+ de 10 Gbps, com operação independente das portas de 1Gbps, permitindo sua utilização tanto para uplink quanto para empilhamento físico (stacking), totalizando no mínimo 52 portas físicas;

2.3. Deve possuir capacidade para encaminhamento de pacotes de no mínimo 130 Mpps (milhões de pacotes por segundo);

2.4. Deve possuir capacidade de comutação total mínima (switching) de 170 Gbps;

2.5. Deve permitir instalação em rack de 19” padrão Telco EIA, incluindo todos os acessórios para fixação, devendo ocupar no máximo 1 (um) rack unit (RU);

2.6. Deve possuir fonte de alimentação interna com ajuste automático de tensão entre 110 e 220V AC, e frequência 50/60 Hz;

2.7. Deve possuir no mínimo 2 (duas) fontes de alimentação internas, redundantes, de mesma capacidade e hot-swappable;

2.8. As fontes em conjunto, devem prover no mínimo, 740 (setecentos e quarenta) Watts de potência para PoE independente da tensão de entrada;

2.9. Deverão ser fornecidos cabos de alimentação para todas as fontes do switch no padrão NBR 14136;

2.10. Possuir módulos de ventilação (Fan Trail) redundantes, com fluxo de ar “Front-to-Back”, internas, Hot-Swap, independentes entre si. Todos os slots de Fan devem estar ocupados;

2.11. Deverá suportar o uso dos transceivers adquiridos nessa solução;

2.12. Deve permitir empilhamento físico ou virtual (cluster) de pelo menos 8 (oito) equipamentos da mesma família e permitir gerenciar a solução como uma única entidade lógica por meio de endereço IP único ou interface de gerência centralizada;

2.13. O equipamento deverá suportar interconexão em pilha ou cluster com capacidade agregada de, no mínimo, 40 Gbps Full Duplex de throughput total por switch;

2.14. Deverão ser fornecidos, junto com cada switch, todos os módulos e cabos necessários para a interconexão em pilha ou cluster. Deve ser entregue com pelo menos 01 (um) cabo de empilhamento de no mínimo 10G com 1 (um) metro de comprimento para redundância na pilha;

2.15. Deve suportar a adição ou retirada de switches na pilha ou cluster sem a interrupção dos outros equipamentos;

2.16. As configurações alteradas deverão ser automaticamente replicadas para todos os membros da pilha ou cluster;

2.17. Deve possuir LEDs indicadores de status de funcionamento, fonte de alimentação, status das portas PoE e indicação de qual switch é o mestre (master) da pilha ou cluster;

2.18. Deve possuir capacidade para armazenar, no mínimo, 2 (duas) imagens distintas do software na memória do equipamento, além de registros de crash (dump) e logs locais;

2.19. O proponente deve apresentar carta oficial de revenda autorizada pelo fabricante do equipamento ofertado;

2.20. Deve ser novo e em plena fabricação. Não serão aceitos equipamentos com avisos de “End of Life” emitidos pelo fabricante;

2.21. Deve possuir certificado de homologação junto à ANATEL;

2.22. Possuir tamanho mínimo da tabela MAC de, no mínimo, 16.000 (dezesseis mil) entradas;

2.23. Implementar tabela ARP para, no mínimo, 3.000 entradas IPv4 e 1.500 entradas IPv6;

2.24. Deve possuir capacidade de configuração de grupos de portas agregadas de acordo com o

protocolo IEEE 802.3ad e IEEE 802.1AX-2008;

2.25. Na criação de grupos de links agregados com portas de diferentes membros da pilha ou cluster, deverá suportar a criação de, no mínimo, 24 grupos por pilha ou cluster;

2.26. Deve suportar o agrupamento de links de, no mínimo, 6 (seis) switches diferentes da pilha ou cluster;

2.27. Deverá suportar a criação de pelo menos 4.000 VLANs, conforme padrão 802.1Q, sendo pelo menos 1.000 VLANs ativas simultâneas;

2.28. Deve implementar os protocolos Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w) e MSTP (Multiple Spanning Tree Protocol);

2.29. Deve implementar Rapid Per-VLAN spanning tree (RPVST+), ou Per-VLAN spanning tree (PVST+), ou VBST (VLAN-Based Spanning Tree), ou protocolo similar em funcionalidade;

2.30. Deve permitir a criação de VLAN específica para voz (voice VLAN) com associação automática;

2.31. Deve suportar Jumbo frames de no mínimo 9018 Bytes;

2.32. Deve implementar o mecanismo IGMP v1/v2/v3 e IGMP snooping/proxy;

2.33. Deve implementar PIM-SM ou PIM-SSM;

2.34. Deve implementar os protocolos LLDP (IEEE 802.3ab) e LLDP-MED, com autonegociação de energia para PoE;

2.35. Deve possuir controle de broadcast, unicast desconhecido e multicast por porta;

2.36. O suporte ao protocolo IPv6 poderá ser evidenciado através da certificação IPv6 Ready Logo ou conformidade com as RFCs: RFC4291, RFC 6724, RFC4443, RFC8200, RFC4862 e RFC4541;

2.37. Deverá permitir a configuração de interfaces virtuais (VLAN Interfaces) para roteamento entre VLANs;

2.38. Deverá implementar o encaminhamento de requisições DHCP (DHCP relay);

2.39. Deve permitir a configuração de rotas estáticas IPv4 e IPv6;

2.40. Deve suportar roteamento dinâmico através do protocolo OSPFv2 e OSPFv3;

2.41. Implementar listas de controle de acesso (ACL) com capacidade de configuração de no mínimo 1.000 ACLs, com processamento em hardware;

2.42. Capacidade de aplicar ACLs para tráfego de entrada e saída em portas de comunicação ou em interfaces de roteamento de VLANs;

2.43. Filtragem de tráfego baseada em: Endereço MAC de origem/destino, Endereço IP de origem/destino, Portas TCP/UDP e tipo de protocolo;

2.44. Deve implementar controle de acesso por porta usando o padrão IEEE 802.1x, com suporte a autenticação via EAP-PEAP, EAP-TLS e EAP-TTLS;

2.45. Deve implementar associação automática de VLAN e aplicação de ACLs ou roles (papéis) na porta através do download do servidor RADIUS/NAC (Change of Authorization - CoA RFC 5176);

2.46. Suportar autenticação 802.1x via endereço MAC (MAB) para dispositivos sem suplicante e autenticação via Portal Web;

2.47. Permitir a autenticação de múltiplos usuários/dispositivos na mesma porta do switch (ex: Telefone IP e PC) em VLANs distintas;

2.48. Implementar controle de acesso para gerenciamento compatível com autenticação TACACS+ e RADIUS;

2.49. Suportar proteção contra ataques “ARP Poisoning”, ARP spoof, DHCP spoof e IP spoof;

2.50. Deve implementar proteção por BPDU (root ou loop);

2.51. Proteção da CPU do switch contra-ataques de negação de serviço (DoS);

2.52. Dar shutdown em uma porta sob broadcast storm;

2.53. Suportar o monitoramento e gerenciamento por meio do protocolo SNMP v1, v2c e v3;

2.54. Deverá permitir o acesso de no mínimo 5 sessões simultâneas para gerenciamento remoto através do protocolo SSH v2;

2.55. Deve permitir o gerenciamento local através de porta console (RJ-45, USB ou similar);

2.56. Deverá implementar a RFC 5424 para envio de mensagens de log (syslog);

2.57. Implementar funcionalidade de provisionamento para configurações automatizadas (Zero Touch Provisioning);

2.58. Deve suportar a sincronização autenticada do relógio interno através do protocolo NTP ou SNTP;

2.59. Deve permitir o monitoramento de tráfego através dos protocolos NetFlow ou IPFIX (RFC 3917) ou NetStream ou SFLOW;

2.60. Permitir o espelhamento de tráfego (Port Mirror) de entrada, saída ou ambos, para porta local ou remota (RSPAN);

2.61. Deverá implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) em nível 2 (IEEE 802.1ag) e nível 3 (ICMP Echo, UDP Jitter);

2.62. Deve implementar 8 (oito) filas de prioridade por porta, permitindo a atribuição de pesos distintos para cada fila;

2.63. Deve executar o processamento do QoS em hardware (Strict Priority e WRR/DRR);

2.64. Classificação baseada em: Porta, IP origem/destino, Portas TCP/UDP, MAC, prioridade 802.1p ou DSCP;

2.65. Permitir o mapeamento e a remarcação de prioridades (802.1p para DSCP e vice-versa);

2.66. Permitir a aplicação de traffic-shaping e rate-limiting;

2.67. Deve suportar a ativação futura de Telemetria;

ITEM 3 - PONTO DE ACESSO SEM FIO – INDOOR

3.1. Deverá ser do mesmo fabricante da SOLUÇÃO DE GERENCIAMENTO, para fins de compatibilidade e suporte unificado;

3.2. Deverá possuir estrutura que permita a utilização do equipamento em locais internos (indoor), com fixação em teto e parede, incluindo todos os acessórios necessários;

3.3. Não serão aceitos equipamentos com padrão de instalação física apenas em parede, conhecidos como “wall plate”, uma vez que a instalação física prioritária deverá ocorrer no teto;

3.4. Deve possuir certificado de homologação junto à ANATEL;

3.5. Deve ser compatível com o padrão Wi-Fi 6 (IEEE 802.11ax) e possuir as funcionalidades: DL/UL OFDMA, MU-MIMO (Múltiplas Entradas e Múltiplas Saídas para Múltiplos Usuários), BSS Coloring e Target Wake Time (TWT);

3.6. Deve suportar, no mínimo, 200 (duzentos) usuários wireless simultâneos por ponto de acesso;

3.7. Deve possuir suporte a pelo menos 8 (oito) SSIDs (WLANs) por ponto de acesso;

3.8. Possibilitar alimentação elétrica local e via padrão Power over Ethernet (padrão IEEE 802.3af ou 802.3at) através de uma única interface de rede, sem perda de funcionalidades e de desempenho;

3.9. Deverá possuir, no mínimo, 1 (uma) interface Ethernet 10/100/1000Base-T (RJ-45) auto-sensing;

3.10. Deverá possuir indicador luminoso (LED) para visualização do status de operação;

3.11. Deverá suportar detecção de pontos de acesso não autorizados (Rogue AP), podendo esta funcionalidade ser provida pela solução de gerenciamento;

3.12. Deve suportar a formação de redes Mesh e ser compatível com IPv4, IPv6 e operação em dual-stack;

3.13. O ponto de acesso deverá atender aos padrões IEEE 802.11a/b/g/n/ac/ac wave 2 e 802.11ax, com operação simultânea em 2.4 GHz e 5 GHz;

3.14. Deverá implementar taxas de transmissão nominais de, no mínimo, 570 Mbps na frequência de 2.4 GHz e de, no mínimo, 1200 Mbps na frequência de 5 GHz, totalizando uma capacidade mínima agregada de 1.7 Gbps;

3.15. Deverá possuir tecnologia de Antenas Inteligentes (Smart Antennas) ou conformação de feixe dinâmica (Beamforming) baseada em hardware, capaz de suprimir interferências e direcionar o ganho de sinal;

3.16. Deverá possuir mecanismo de rádio com configuração de antenas de, no mínimo, 2x2:2 MIMO (spatial streams) em ambas as frequências (2.4 GHz e 5 GHz);

3.17. Deverá suportar potência agregada de saída (Tx Power) de, no mínimo, 23 dBm nas frequências de 5 GHz e de 2.4 GHz, com sensibilidade de recepção de no mínimo -95 dBm (ou superior);

3.18. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz;

3.19. Deve permitir ajustes dinâmicos do sinal de rádio frequência (RRM) e seleção automática de canal (DCA/DFS);

3.20. Deve suportar os padrões de roaming rápido e gerenciamento de rádio IEEE 802.11r, IEEE 802.11k e IEEE 802.11v;

3.21. A solução deverá contemplar funcionalidade de controle de acesso à rede (NAC), integrada ou interoperável, permitindo autenticação, autorização e contabilização (AAA) com base em identidade, perfil e contexto;

3.22. A solução deverá incluir, integrada ao preço do equipamento e sem custos adicionais, a licença e o software da plataforma de gestão de usuários e controle de acesso para convidados;

3.23. Deverá permitir a criação de Portal Captivo (Captive Portal) customizável com a logomarca do Ministério e termos de uso;

3.24. Deverá suportar autenticação via portal cativo, incluindo opções como voucher, e-mail, SMS ou integração com serviços externos;

3.25. Deverá permitir o fluxo de aprovação por patrocinador (Sponsor-based), onde um servidor do órgão autoriza o acesso do visitante via interface web ou e-mail;

3.26. Deverá permitir a gestão de tempo de conexão, com definição de limite máximo de uso diário e tempo de inatividade;

3.27. Deverá suportar autenticação 802.1X (EAP-PEAP, EAP-TLS) e autenticação via endereço MAC (MAB);

3.28. Deverá permitir a integração nativa com serviços de diretório e autenticação externos (RADIUS, LDAP e Microsoft Active Directory) e implementar mecanismos de cache de autenticação (Fast Roaming), visando garantir a reconexão automática e de baixa latência durante o deslocamento de dispositivos entre diferentes Access Points da solução;

3.29. Deverá suportar a criação de chaves pré-compartilhadas privadas (PPSK ou iPSK), permitindo senhas únicas por dispositivo em um mesmo SSID;

3.30. Deverá suportar identificação de aplicações em camada 7, permitindo aplicação de políticas de controle e limitação de banda por usuário, grupo ou SSID;

3.31. Deverá permitir a visualização de gráficos e relatórios de acessos, informando fabricante do dispositivo, sistema operacional e volume de dados trafegados;

3.32. Deverá permitir geração de logs detalhados e integração com sistemas externos de monitoramento e ferramentas de análise de eventos de segurança (SIEM);

3.33. Deverá permitir integração com sistemas externos via WebService REST/API;

3.34. Deve permitir que sua configuração e atualização de software sejam realizadas automaticamente (Zero Touch Provisioning) através da SOLUÇÃO DE GERENCIAMENTO centralizada;

3.35. A solução deverá permitir gerenciamento centralizado e unificado da rede sem fio, com aplicação consistente de políticas de acesso e segurança;

3.36. Deverá implementar, no mínimo, os seguintes padrões de segurança: WPA2-AES, WPA3 (Personal e Enterprise) e IEEE 802.11i;

3.37. Em caso de falha de comunicação com a gerência central, os usuários já autenticados devem permanecer conectados (Survivability), e novos usuários devem conseguir se autenticar via RADIUS local se configurado;

ITEM 4 - TRANSCEIVER SFP+ 10G

4.1. Transceiver SFP+, padrão 10GE Base-SR, fibra multimodo, até 300 metros;

4.2. O módulo transceiver deverá ser perfeitamente compatível e acompanhar a garantia dos switches a serem adquiridos no objeto (itens 1 e 2);

4.3. Serão aceitos transceivers de fabricantes distintos aos dos switches, desde que possuam homologação de pleno funcionamento com os equipamentos ofertados, não sendo admitidos módulos que causem instabilidade ou recusa de tráfego;

ITEM 5 - SOLUÇÃO DE GERENCIAMENTO

5.1. A solução de rede local (switches) e a solução de rede sem fio (pontos de acesso) deverão ser gerenciadas por um único ecossistema de gerenciamento centralizado, permitindo a orquestração de políticas, correlação de eventos e monitoramento unificado por meio de interface gráfica ou conjunto de ferramentas integradas do mesmo fabricante;

5.2. Por questões de compatibilidade técnica, garantia de performance da gerência unificada, suporte técnico único e integração nativa, a Solução de Gerenciamento deve ser do mesmo fabricante dos Switches e dos Pontos de Acesso;

5.3. Deve suportar nativamente a arquitetura de múltiplos sites (Multi-Site), permitindo a criação de uma estrutura hierárquica lógica (ex: Organização > Ministério > Prédio > Andar) com aplicação de configurações globais e locais de forma independente;

5.4. A solução de gerenciamento deverá ser dimensionada para suportar o gerenciamento de no mínimo 512 (quinhentos e doze) pontos de acesso e o tráfego de 5.000 (cinco mil) dispositivos simultâneos;

5.5. A solução de gerenciamento deverá atuar como a plataforma central de controle e orquestração (seja via Controladora Física, Virtual ou em Nuvem);

5.6. A solução pode ser fornecida como appliance virtual compatível com o hypervisor existente

Nutanix AHV e AOS, em versão 10.3 ou superior, ou como appliance físico. No caso de appliance virtual, cabe à contratada assegurar a compatibilidade com o ambiente Nutanix ou fornecer o hardware necessário. Para appliance físico, a contratada deve prover todo o hardware e software requeridos para o pleno funcionamento;

5.7. Caso a solução ofertada necessite de hardware (Appliance, Servidor ou Controladora WLC), este deverá ser fornecido e dimensionado com redundância (Alta Disponibilidade) conforme as especificações técnicas descritas nos subitens abaixo:
5.7.1. Possuir componentes necessários para a instalação em rack 19" 1RU.

5.7.2. Possuir fontes de alimentação, 110-220V, 50/60Hz, e módulos de ventilação redundantes (Hot-Swap);

5.7.3. Possuir conectividade mínima 08 (oito) portas SFP+ 10Gbps ou 02 (duas) portas QSFP+ 40Gbps, com capacidade de agregação de links;

5.8. Independente da modalidade de entrega, a solução deve garantir acesso remoto seguro via HTTPS e o pleno funcionamento do Zero Touch Provisioning (ZTP) e da coleta de telemetria, operando mesmo através de NAT ou túneis VPN;

5.9. Deve realizar o backup automático, controle de versão das configurações e permitir a atualização programada de firmware dos ativos (Switches e APs) de forma centralizada, sem necessidade de intervenção local;

5.10. Deve possuir funcionalidade de gerência de rádio (RRM) para prover automação de potência e canal de operação através da análise do ambiente de RF em tempo real, mitigando interferências e provendo estabilidade à rede sem fio;

5.11. O Dashboard deve fornecer um índice de integridade da rede, classificando incidentes por severidade e fornecendo informações detalhadas para diagnóstico e correção de falhas;

5.12. A solução deve monitorar a saúde dos serviços essenciais de rede, identificando falhas e latências em: Associação Wi-Fi, Autenticação (802.1X), tempo de resposta de DHCP, resolução de DNS e latência de servidores RADIUS;

5.13. Deve fornecer visibilidade de aplicações (Camada 7), permitindo identificar o consumo de banda por protocolo ou aplicação e permitir a aplicação de políticas de QoS ou restrição de tráfego;

5.14. Deve permitir a realização de diagnósticos remotos (Troubleshooting) como Ping, Traceroute e verificação de integridade de cabos (TDR), permitindo a visualização do status de todos os ativos de rede, incluindo alertas de falhas e utilização de CPU/Memória;

5.15. O licenciamento deve cobrir todos os custos de funcionamento da plataforma, hardware de gerência (se houver), processamento e armazenamento de dados pelo período de 60 (sessenta) meses;

5.16. A subscrição deve incluir suporte técnico do fabricante em regime 24x7, com direito a todas as atualizações de software e patches de segurança lançados durante a vigência contratual;

5.17. Independente do modelo comercial adotado pelo fabricante (licenciamento por dispositivo, por nó ou por plataforma centralizada), a solução deve ser entregue com o licenciamento necessário para o gerenciamento pleno da totalidade dos ativos adquiridos (Switches e pontos de acesso). O licenciamento fornecido deve habilitar a plenitude dos recursos de gerência, segurança, automação e telemetria exigidos neste Termo de Referência, sendo vedada a entrega de licenças de categorias reduzidas ou parciais que limitem as funcionalidades nativas ou integradas dos equipamentos;

5.18. Visando permitir a participação de soluções que operem sob arquiteturas unificadas ou convergentes, as funcionalidades exigidas neste item poderão ser providas pela Solução de Gerenciamento, pela Solução de Controle de Acesso (NAC) ou pela integração técnica entre ambas, desde que pertençam ao mesmo ecossistema do fabricante e garantam o atendimento integral dos requisitos técnicos e operacionais descritos;

ITEM 6 - PLATAFORMA DE CONTROLE DE ACESSO À REDE (NAC)

6.1. A solução de Controle de Acesso à Rede (NAC) deverá estar integrada ao mesmo ecossistema de rede, permitindo a orquestração de identidades, automação de políticas de acesso e visibilidade de dispositivos (profiling) de forma unificada, por meio de interface integrada do mesmo fabricante dos Switches e dos Pontos de Acesso;

6.2. Por questões de interoperabilidade nativa, garantia de performance na aplicação de políticas de segurança, suporte técnico único e evolução coordenada das funcionalidades entre a infraestrutura e a camada de controle, a Plataforma NAC deve ser obrigatoriamente do mesmo fabricante dos Switches e dos Pontos de Acesso;

6.3. Não serão aceitos sistemas baseados exclusivamente em software de código aberto (open source) de uso genérico, devendo a solução possuir suporte direto do fabricante;

6.4. Deverá ser capaz de realizar o controle de acesso para no mínimo 5.000 (cinco mil)

dispositivos simultâneos, abrangendo estações de trabalho, impressoras, telefones IP, Access Points e dispositivos IoT;

6.5. A solução pode ser fornecida como appliance virtual compatível com o hypervisor existente Nutanix AHV e AOS, em versão 10.3 ou superior, ou como appliance físico. No caso de appliance virtual, cabe à contratada assegurar a compatibilidade com o ambiente Nutanix ou fornecer o hardware necessário. Para appliance físico, a contratada deve prover todo o hardware e software requeridos para o pleno funcionamento.

6.6. Deverá suportar a integração nativa com diretórios de identidade corporativos (Active Directory / LDAP) para a autenticação segura de usuários;

6.7. Implementar autenticação baseada no protocolo IEEE 802.1X para redes cabeadas e sem fio, além de suportar MAC Authentication Bypass (MAB) para dispositivos que não suportam 802.1X;

6.8. Capacidade de identificar e classificar dispositivos de modo automatizado através de técnicas como HTTP User-Agent, MAC OUI, DHCP e escaneamento via NMAP, permitindo a criação de perfis automáticos (Profiling);

6.9. Implementar Controle de Postura e Conformidade (Posture), permitindo validar o status de segurança dos dispositivos (ex: antivírus ativo, patches de SO) e aplicar quarentena ou bloqueio em caso de não conformidade;

6.10. Deve incluir funcionalidade de Portal Cativo (Captive Portal) para visitantes, suportando auto-registro, aprovação por patrocinador (Sponsor-based), uso de vouchers e termos de uso personalizáveis;

6.11. Implementar o mecanismo de Change of Authorization (CoA - RFC 5176), permitindo alterar dinamicamente a permissão de um usuário já autenticado em caso de violação de política detectada;

6.12. Garantir a segmentação dinâmica de tráfego (VLANs/ACLs) baseada no perfil de autenticação e política de QoS associada ao usuário ou dispositivo;

6.13. A geração e armazenamento de trilhas de auditoria (logs) devem conter obrigatoriamente a identificação do evento, data/hora, usuário, endereço IP e endereço MAC do dispositivo;

6.14. Implantar funcionalidades de relatórios gráficos, incluindo o fabricante do dispositivo, tipo do dispositivo, endereçamento IP, políticas em uso aplicada, sistema operacional e regras de Controle de Acesso associada;

6.15. Possuir licenciamento para uso permanente/perpétuo ou em modalidade de subscrição pelo período de 60 (sessenta) meses;

6.16. A subscrição deve incluir suporte técnico do fabricante em regime 24x7 e acesso a todas as atualizações de software e segurança durante o período de vigência;

6.17. Visando permitir a participação de soluções que operem sob arquiteturas unificadas ou convergentes, as funcionalidades exigidas neste item poderão ser providas pela Solução de Gerenciamento, pela Solução de Controle de Acesso (NAC) ou pela integração técnica entre ambas, desde que pertençam ao mesmo ecossistema do fabricante e garantam o atendimento integral dos requisitos técnicos e operacionais descritos;

7. CONDIÇÕES GERAIS DE EXECUÇÃO DOS SERVIÇOS DE GARANTIA E SUPORTE

7.1. A CONTRATADA deverá fornecer garantia integral e suporte técnico especializado para todos os ativos de rede (hardware e software) pelo período mínimo de 60 (sessenta) meses, contados a partir do recebimento definitivo da solução;

7.2. Todas as peças, módulos e componentes substituídos durante o período de garantia deverão ser deverão ser originais, de padrão tecnológico igual ou superior, em pleno estado de funcionamento e com garantia integral pelo fabricante, mantendo a total compatibilidade com a solução implantada;

7.3. O suporte técnico deverá ser prestado diretamente pelo fabricante ou por parceiro técnico devidamente autorizado e certificado, em regime de disponibilidade 24x7 (vinte e quatro horas por dia, sete dias por semana);

7.4. NÍVEIS DE ATENDIMENTO TÉCNICO

7.5. O suporte técnico será estruturado em 3 (três) níveis de atendimento, conforme as necessidades e a complexidade do incidente:

7.6. Nível I - Atendimento Telefônico (Help Desk): Destinado ao primeiro contato para registro de incidentes, esclarecimento de dúvidas operacionais e suporte básico. O CONTRATANTE deverá ter acesso a um canal de atendimento (0800 ou similar) e portal web para abertura e acompanhamento de chamados, devendo todos os canais de atendimento serem disponibilizados obrigatoriamente em idioma Português (Brasil);

7.7. Nível II - Atendimento Remoto: Consiste na intervenção técnica realizada através de acesso remoto seguro à infraestrutura do MCID. Este nível destina-se a diagnósticos avançados, ajustes de configuração, atualizações de sistema e resolução de problemas lógicos que não exijam

intervenção física;

7.8. Nível III - Atendimento Presencial (On-Site): Destinado à resolução de falhas que exijam a presença física de técnico especializado nas dependências do Ministério em Brasília/DF. Este nível inclui a substituição física de hardware (switches, transceivers ou pontos de acesso), correções de segurança, atualizações de software/firmware, e a reconfiguração presencial dos ativos para o restabelecimento imediato dos serviços, sem qualquer ônus adicional para o Ministério;

7.9. NÍVEIS MÍNIMOS DE SERVIÇO (SLA) E SEVERIDADES

7.10. Todo chamado deverá ser registrado inicialmente via Nível I (Help Desk), sendo o acionamento dos níveis subsequentes (Remoto ou Presencial) determinado pela complexidade do incidente ou pela impossibilidade de resolução no primeiro contato;

7.11. A CONTRATADA deverá classificar e atender aos chamados de acordo com os seguintes níveis de severidade:

7.11.1. SEVERIDADE CRÍTICA: Aplicada quando a solução ou parte essencial dela estiver inoperante, impedindo a continuidade das atividades do Ministério. O atendimento deverá ser iniciado em até 04 (quatro) horas corridas; e o prazo para solução/contorno é de até 24 (vinte e quatro) horas corridas;

7.11.2. SEVERIDADE ALTA: Aplicada em incidentes que causem dano moderado ou interrupções recorrentes em funcionalidades importantes, sem a paralisação total da rede. O atendimento deverá ser iniciado em até 08 (oito) horas corridas; e o prazo para solução/contorno é de até 48 (quarenta e oito) horas corridas;

7.11.3. SEVERIDADE MÉDIA: Aplicada em falhas que causem redução de performance intermitente ou erros em recursos não essenciais, permitindo a operação da rede com limitações. O atendimento deverá ser iniciado em até 12 (doze) horas corridas; e o prazo para solução/contorno é de até 72 (setenta e duas) horas corridas;

7.11.4. SEVERIDADE BAIXA OU INFORMATIVA: Aplicada para dúvidas de configuração, solicitações de relatórios, dashboards ou incidentes de baixo impacto que não afetem a performance da rede. O atendimento deverá ser iniciado em até 24 (vinte e quatro) horas corridas; e o prazo para solução/contorno é de até 05 (cinco) dias úteis;

7.12. Em caso de necessidade de substituição física de hardware (Nível III), o novo equipamento deverá estar instalado e operacional no prazo máximo de NBD (Next Business Day – Próximo Dia Útil), contado a partir da confirmação do defeito físico pela equipe de Nível II;

7.13. Um chamado técnico somente será considerado encerrado mediante a confirmação formal da CONTRATANTE de que o recurso foi restabelecido e encontra-se em perfeitas condições de funcionamento;

7.14. Caso a falha seja decorrente de elementos externos não fornecidos pela CONTRATADA, os prazos de SLA serão suspensos até que o ambiente seja devidamente estabilizado pela CONTRATANTE;

7.15. ATUALIZAÇÃO E SUSTENTAÇÃO

7.16. Durante toda a vigência da garantia, o CONTRATANTE terá direito ao download e instalação de todas as novas versões de software, correções de bugs (patches) e atualizações de segurança disponibilizadas pelo fabricante para os ativos adquiridos;

7.17. A CONTRATADA deverá notificar proativamente o Ministério sobre a disponibilidade de atualizações críticas que visem mitigar vulnerabilidades de segurança na infraestrutura de rede;

7.18. VISIBILIDADE E MONITORAMENTO

7.19. A Contratada deverá fornecer e implantar solução de visualização de dados (Dashboards), de forma centralizada, permitindo o monitoramento executivo e técnico de performance, segurança e operação de toda a infraestrutura objeto deste termo;

7.19.1. A solução poderá ser disponibilizada em modalidade sob nuvem (SaaS) ou instalada localmente (On-premise), garantindo o acesso via interface Web segura (HTTPS);

7.19.2. É de responsabilidade da CONTRATADA a configuração e manutenção de painéis com indicadores de prontidão, de modo que a CONTRATANTE disponha de visões prontas para consumo imediato após a implantação;

7.19.3. O acesso aos painéis deve possuir controle por perfil de usuário, suportando autenticação multifator (MFA) e mecanismos de recuperação de senha via e-mail;

7.19.4. A interface de visualização deve ser do tipo responsiva, garantindo a integridade da exibição em diferentes tamanhos de tela e dispositivos (monitores, notebooks e tablets);

7.19.5. A plataforma deve permitir a visualização de indicadores através de múltiplos elementos gráficos (como medidores de KPI, gráficos de barras, linhas, setores e tabelas dinâmicas), permitindo a correta interpretação de dados em tempo real e históricos;

7.19.6. Deve possuir recursos de filtragem avançada e customizável, permitindo a segmentação de

dados por período (dia, semana, mês, ano), localidade física, tipo de dispositivo e severidade de eventos;

7.19.7. Permitir a exportação dos relatórios e painéis em formatos padrão de mercado (como PDF, CSV ou imagem), para fins de instrução de processos e auditoria;

7.19.8. A solução deve suportar a coleta automática e recorrente de dados provenientes dos ativos de rede (Switches e pontos de acesso) e da plataforma de gerência/NAC, garantindo a atualização constante dos indicadores sem necessidade de intervenção manual;

ANEXO II MODELO DE PROPOSTA

MODELO DE PROPOSTA

PREGÃO ELETRÔNICO Nº XX/2026 - MCID

DADOS DA EMPRESA	
1. Razão Social da Empresa:.....	2. CNPJ nº: .....
3. Inscrição Estadual:	4. Inscrição Municipal: .....
5. Endereço Completo.....	6. Telefone: (XX)..... E-mail: .....
7. Banco: ..... Agência: ..... Conta Corrente:	8. Representante da Empresa: .....
9. Cargo:	10. Optante pelo SIMPLES: ( ) Sim ( ) Não

Apresentamos nossa proposta para a contratação de ativos de infraestrutura de TIC visando atender às necessidades presentes e futuras do Ministério das Cidades:

LOTE 01							
ITEM	**DESCRIÇÃO**	**FABRICANTE / PART NUMBER**	**CATMAT/CATSER**	**MÉTRICA OU UNIDADE DE MEDIDA**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL POR ITEM**
1	Switch de núcleo		393273	Unidade	4		
2	Switch de acesso		393274	Unidade	50		
3	Ponto de acesso sem fio - Indoor		404260	Unidade	125		
4	Transceiver SFP+ 10G		618351	Unidade	100		
5	Solução de Gerenciamento		27014	Unidade	1		
6	Plataforma de Controle de Acesso à Rede (NAC)		27022	Unidade	1		
VALOR TOTAL							

Prazo de validade da proposta: ____ dias (não inferior a 60 dias).

Local e data

_____

Assinatura (representante legal)

ANEXO III - TERMO DE CIÊNCIA

TERMO DE CIÊNCIA

INTRODUÇÃO
O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão. No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar aos Fiscais do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados. **Referência: Art. 18, Inciso V, alínea "b" da IN SGD/ME Nº 94/2022.**

1 - IDENTIFICAÇÃO			
CONTRATO Nº	<xxxx/aaaa>		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	**CNPJ**	<xxxxxxxxxx>
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	**MATR.**	<xxxxxxxxxx>

2 - CIÊNCIA
Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

FUNCIONÁRIOS DA CONTRATADA	
NOME	**ASSINATURA**
<Nome do(a) Funcionário(a)>	
<Nome do(a) Funcionário(a)>	

ANEXO IV - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <Nº do CNPJ>, doravante denominada **CONTRATADA.**

CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE.**

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção.

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade do **CONTRATANTE.**

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO,** doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 - OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pelo CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 - CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 - DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 - DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I - sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II - tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III - sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 - DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 - VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 - PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

8 - DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro - Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé,

da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo - O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I - O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II - A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III - A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV - Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V - O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI - Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII - O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII - Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 - FORO

O CONTRATANTE elege o foro da Brasília, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 - ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado eletrônicamente pela partes e testemunhas.

CONTRATADA	**CONTRATANTE**
_____ <Nome> <Qualificação>	_____ <Nome> **Matrícula:** xxxxxxxx

TESTEMUNHAS	
_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>

ANEXO V - MODELO DE ORDEM DE SERVIÇO (OS)

MODELO DE ORDEM DE SERVIÇO (OS)

INTRODUÇÃO
Por intermédio da Ordem de Serviço (OS) será solicitado formalmente à Contratada a prestação de serviço relativos ao objeto do contrato. O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os serviços estejam compreendidos dentro do prazo de vigência contratual. **Referência: Art. 32 IN SGD Nº 94/2022.**

1 - IDENTIFICAÇÃO			
Nº da OS/OFB	<xx/aaaa>	**Data de emissão**	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO nº	<xx/aaaa>		
Objeto do Contrato	<Descrição do objeto do contrato>		
Contratada	<Nome da contratada>	**CNPJ**	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	**Fim vigência**	<dd/mm/aaaa>
ÁREA REQUISITANTE			
Unidade	< Sigla – Nome da unidade>		
Solicitante	<Nome do solicitante>	**E-mail**	<xxxxxxxxxxxxx@cidades.gov.br>

2 - ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES ESTIMADOS

ITEM	DESCRIÇÃO	CATÁLOGO	MÉTRICA OU UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL POR ITEM
1	Switch de Núcleo	CATMAT 393273	Unidade		R$	R$
2	Switch de Acesso	CATMAT 393274	Unidade		R$	R$
3	Ponto de acesso sem fio - Indoor	CATMAT 404260	Unidade		R$	R$
4	Transceiver SFP+ 10G	CATMAT 618351	Unidade		R$	R$
5	Solução de Gerenciamento	CATSER 27014	Unidade		R$	R$
6	Plataforma de Controle de Acesso à Rede (NAC)	CATSER 27022	Unidade		R$	R$
VALOR TOTAL					R$	

3 - INSTRUÇÕES/ESPECIFICAÇÕES COMPLEMENTARES

4 - DATAS E PRAZOS PREVISTOS			
Data de Início:	<dd/mm/aaaa>	**Data do Fim:**	<dd/mm/aaaa>
CRONOGRAMA DE EXECUÇÃO/ENTREGA			
ITEM	**TAREFA/ENTREGA**	**INÍCIO**	**FIM**
1			
2			
3			
4			
5			
6			
7			
8			

5 - ASSINATURA E ENCAMINHAMENTO DA DEMANDA	
Autoriza-se a execução dos serviços correspondentes à presente OS, no período e nos quantitativos acima identificados.	
_____ <Nome > **<Responsável pela demanda/ Fiscal Requisitante>** Matr.: <Nº da matrícula>	_____ <Nome > **Gestor do Contrato** Matr.: <Nº da matrícula>

ANEXO VI - MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

INTRODUÇÃO
O Termo de Recebimento Provisório trata-se de termo detalhado que declarará que os serviços foram prestados e atendem às exigências de caráter técnico, sem prejuízo de posterior verificação de sua conformidade com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato. **Referência: Inciso XXI, art. 2º, e alínea "i", inciso II, art. 33 da IN SGD/ME Nº 94/2022.**

1 - IDENTIFICAÇÃO			
CONTRATO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 - ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**
1	<Descrição igual ao da OS de abertura>	<Ex.: PF>	<n>
…	…	…	…
…	…	…	…
…	…	…	…
TOTAL DE ITENS			

3 - RECEBIMENTO
Para fins de cumprimento do disposto no art. 33, inciso II, alínea "i", da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os serviços correspondentes à <OS> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram executados e <atende(m)/atende(m) parcialmente/não atende(m)> às respectivas exigências de caráter técnico discriminadas abaixo. Não obstante, estarão sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato. Ressaltamos que o recebimento definitivo desses serviços ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

ITEM	**ESPECIFICAÇÃO TÉCNICA**	**ATENDIMENTO**	**OBSERVAÇÃO**
1	<exigências técnicas definidas no TR>	...	.....
…	…	…	.....
…	…	…	.....
…	…	…	.....

4 - ASSINATURA
FISCAL TÉCNICO

4 - ASSINATURA
_____ <Nome do Fiscal Técnico do Contrato> **Matrícula:** xxxxxx <Local>, <dia> de <mês> de <ano>.
PREPOSTO
_____ <Nome do Preposto do Contrato> **Matrícula**: xxxxxx <Local>, <dia> de <mês> de <ano>.

ANEXO VII - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelelcidos. **Referência: Inciso XXII, Art. 2º e alínea "h" inciso I do art. 33, da IN SGD/ME Nº 94/2022.**

1 - IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	**CNPJ**	xxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 - ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	**DESCRIÇÃO DO BEM OU SERVIÇO**	**MÉTRICA**	**QUANTIDADE**	**TOTAL**
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
…				
TOTAL DE ITENS				

3 - ATESTE DE RECEBIMENTO

3 - ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea "h", da IN SGD/ME nº 94/2022, por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	.....
…	…	…	.....
…	…	…	.....
…	…	…	.....

4 - DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos. <Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>. Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 - ASSINATURA

GESTOR DO CONTRATO

_____
<Nome do Gestor do Contrato>
Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>.

<As seções seguintes podem constar em documento diverso, pois dizem respeito à autorização para o faturamento, a cargo do Gestor do Contrato, e a respectiva ciência do preposto quanto a esta autorização>.

6 - AUTORIZAÇÃO PARA FATURAMENTO

GESTOR DO CONTRATO

Nos termos da alínea "n", inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima.

_____
<Nome do Gestor do Contrato>
Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>

7 - CIÊNCIA

PREPOSTO

_____
<Nome do Preposto do Contrato>
Matrícula: xxxxxxx

<Local>, <dia> de <mês> de <ano>

ANEXO VIII - MODELOS DE TERMOS DE VISTORIA

MODELOS DE TERMOS DE VISTORIA

A) MODELO DE TERMO DE VISTORIA

TERMO DE VISTORIA

A empresa <NOME DA EMPRESA> , sediada na <endereçço> , CNPJ n° <CNPJ>, declara que lhe foi concedido acesso a dependências do Ministério das Cidades (MCID), bem como que lhe foram esclarecidas todas as questões por ela suscitadas, e, ainda, que tem pleno conhecimento das condições técnicas e materiais relacionadas à execução de todos os serviços objetos do Pregão Eletrônico nº <___/2026 -MCID.

<Local>, <datapor extenso>.

Representante
<Nome do representante legal ou procurador>

De acordo.

Fiscal técnico
<Nome do Servidor> Siape: <matrícula>

OU

B) MODELO DE DECLARAÇÃO DE CONHECIMENTO DAS CONDIÇÕES DE EXECUÇÃO E RENÚNCIA À VISTORIA

DECLARAÇÃO DE CONHECIMENTO DAS CONDIÇÕES DE EXECUÇÃO E DE RENÚNCIA À VISTORIA

A empresa <NOME DA EMPRESA> , sediada na <endereço> , CNPJ n° <CNPJ> , por ocasião de participação no Pregão Eletrônico < ___/2026 - MCID, **DECLARA** que possui pleno conhecimento das condições de execução e natureza dos serviços objetos do certame em pauta, tendo coletado informações acerca dos elementos necessários e suficientes à adequada elaboração da proposta comercial.

Declara ainda que optou por não realizar vistoria nos locais de prestação, assumindo inteiramente a responsabilidade ou consequências por essa decisão, mantendo as garantias que

vinculam a respectiva proposta ao presente processo licitatório.

<Local>, <data por extenso>.

Representante
<Nome do representante legal ou procurador>

Observações: A empresa licitante deverá, por ocasião do encaminhamento da proposta, apresentar declaração de acordo com um dos modelos apresentados (A ou B), conforme a opção pela realização ou não de vistoria, com os dados da empresa e do declarante, podendo elaborar documento em modelo próprio, desde que contenha a declaração explícita e todos os dados pertinentes.

ANEXO IX - HISTÓRICO DE GESTÃO DO CONTRATO

HISTÓRICO DE GESTÃO DO CONTRATO

INTRODUÇÃO
Através do Histórico de Gestão do Contrato serão documentados os principais pontos/acontecimentos, positivos ou negativos, que ocorreram durante a execução do contrato, organizados por ordem temporal. Este documento poderá servir de insumo para a atualização do Mapa de Gerenciamento de Riscos e para subsidiar o Gestor do Contrato para fins de renovação contratual. **Referências: Arts. 33, inciso I, alínea "k" e 36 IN SGD/ME Nº 94/2022.**

1 – IDENTIFICAÇÃO			
CONTRATO Nº	XXXX/AAAA		
CONTRATADA	<nome da contratada>	**CNPJ**	XXXXXXX
INÍCIO VIGÊNCIA	<DD/MM/AAAA>	**FIM VIGÊNCIA**	<DD/MM/AAAA>
SOLUÇÃO DE TIC	<Objeto do contrato>		

2 – REGISTRO DE EVENTOS	
<data>	<Nome do evento>
…	…
Exemplo:	
21/05/25	Realização da Reunião Inicial.

25/05/25	Realização de reunião de transferência de conhecimento das áreas de negócio para a empresa contratada.
27/05/25	Liberação de acesso aos recursos computacionais para os funcionários da contratada (e-mail, ferramenta de gestão de demandas, etc.).
…	…
02/08/25	Abertura do processo administrativo sancionador, considerando a aplicabilidade de sanções decorrentes do não atingimento dos indicadores de níveis de serviço de junho/2025, apresentados no Relatório de Fiscalização nº 3/2025.

3 – PONTOS DE MELHORIA	
1	<Descrição dos pontos que foram observados como deficientes e que devem ser melhorados neste tipo de contratação>.
…	…

4 – BOAS PRÁTICAS OBSERVADAS NA CONTRATAÇÃO	
1	<Descrição dos pontos positivos na execução do contrato e que podem ser considerados com boas práticas neste tipo de contratação>.
…	…

5 – ASSINATURA

< Conforme art. 33, inciso I, alínea “k” da IN SGD/ME nº 94/2022, o Histórico de Gestão do Contrato é de responsabilidade do Gestor do Contrato, mas todos os fiscais do contrato o apoiam nesta tarefa.

Assim, o documento poderá conter as assinaturas de todos os integrantes da Equipe de Fiscalização do Contrato, a critério dos procedimentos adotados no órgão/entidade.

Este registro pode ser realizado com o apoio de ferramenta computacional, assim como também pode constar em seção específica em Relatório de Fiscalização do Contrato>.

_____

<Nome>

Gestor do Contrato

Matr.: <Nº da matrícula>

Local, xx de xxxxx de xxxx.