ANEXO I - TERMO DE REFERÊNCIA

1. Objeto

Contratação de empresa prestadora dos serviços de operação, atualização das soluções, gerenciamento, monitoramento, treinamento, suporte técnico, manutenção preventiva e manutenção corretiva de toda a infraestrutura de rede de dados (wired e wireless), segurança, controle de acesso, nobreaks e gerador na Fundação de Amparo à Pesquisa do Estado de Minas Gerais - FAPEMIG, conforme especificações técnicas e condições comerciais previstas no Edital e em seus Anexos.

ITEM	CÓDIGO	DESCRIÇÃO	TOTAL
1	-	Serviços de operação, atualização das soluções, gerenciamento, monitoramento, treinamento, suporte técnico, manutenção preventiva e manutenção corretiva de toda a infraestrutura de rede de dados (wired e wireless), segurança, controle de acesso, nobreaks e gerador.	01

Tabela 1: Descrição do item

1.1. Especificação do objeto

Será de total responsabilidade da CONTRATADA a execução dos serviços de operação, atualização das soluções, gerenciamento, monitoramento, treinamento, suporte técnico, manutenção preventiva e manutenção corretiva de toda a infraestrutura de rede de dados (wired e wireless), segurança, controle de acesso, nobreaks e gerador na Fundação de Amparo à Pesquisa do Estado de Minas Gerais – FAPEMIG.

Além das especificações, apresentadas neste termo de referência, dos serviços a serem prestados, deverão ser observadas aquelas apresentadas na especificação técnica e funcional dos equipamentos e softwares que compõe a infraestrutura de TIC, conforme Anexo II - ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE MONITORAMENTO E GERENCIAMENTO e Anexo III – ESPECIFICAÇÕES DOS ATIVOS DE REDE, independente de transcrição.

1.2. Informações complementares

1.2.1. Glossário

- **ACORDO DE NÍVEL DE SERVIÇO (ANS) OU *SERVICE LEVEL AGREEMENT* (SLA):** Acordo firmado entre a área de TI e seu cliente interno, que descreve o serviço de TI, suas metas de nível de serviço, além dos papéis e responsabilidades das partes envolvidas no acordo. Os números que expressam o atendimento esperado dos incidentes. Os índices de atendimento registrados abaixo desses números são considerados insatisfatórios e devem resultar em sanções, conforme o Edital.
- **CMDB (Configuration Management Database):** Banco de dados usado para armazenar os Registros de Configuração durante todo o seu Ciclo de Vida. O Sistema de Gerenciamento da Configuração mantém um ou mais CMDBs, e cada CMDB armazena atributos de ICs (Itens de Configuração) e seus relacionamentos com outros ICs.
- ***COLOCATION*:** Compartilhamento de localização, entendida como espaço físico e infraestrutura.
- **COR:** Centro de Operações de Rede.
- **COS:** Centro de Operações de Segurança.
- **GESTOR DO CONTRATO:** Representante da CONTRATANTE responsável pelo gerenciamento do contrato.
- **INCIDENTE:** Qualquer ocorrência que gere um atendimento de suporte ou de manutenção. Os incidentes devem ser registrados em sistema pela Central de Serviços. O sistema deverá gerar um número de registro do incidente para rastreamento.
- **INFRAESTRUTURA DE TIC:** Conjunto de equipamentos e softwares que compõe a Infraestrutura de Rede de Dados da FAPEMIG.
- **ITEM DE CONFIGURAÇÃO (IC):** Qualquer componente que necessite ser gerenciado para que possa entregar um Serviço de TI. A informação sobre cada IC é registrada no CMDB dentro do Sistema de Gerenciamento da Configuração e é mantida durante todo o seu Ciclo de Vida pelo Gerenciamento da Configuração. ICs estão sob controle do Gerenciamento de Mudanças. ICs tipicamente incluem hardware, software, instalações, pessoas e documentos formais tais como documentos de Processos e ANSs.
- **ITIL:** *Information Technology Infrastructure Library*. É uma biblioteca de boas práticas (do inglês *best practices*) nos serviços de tecnologia da informação

(TI), desenvolvida pela CCTA (*Central Computer and Telecommunications Agency*) e atualmente sob custódia da OGC (*Office for Government Commerce*) da Inglaterra. A ITIL busca promover a gestão com foco no cliente e na qualidade dos serviços de tecnologia da informação (TI). A ITIL endereça estruturas de processos para a gestão de uma organização de TI apresentando um conjunto abrangente de processos e procedimentos gerenciais, organizados em disciplinas, com os quais uma organização pode fazer sua gestão tática e operacional em vista de alcançar o alinhamento estratégico com os negócios. Para essa contratação, deve-se considerar e utilizar a ITIL no mínimo em sua versão 2.0.

- **NAC (*Network Admission Control/Network Access Control*):** Método de reforçar a segurança de uma rede de computadores, restringindo o acesso aos recursos da rede somente aos dispositivos que estejam em conformidade com uma política de segurança definida pela CONTRATANTE.
- **PROBLEMA:** A causa desconhecida de um ou mais incidentes. Um problema é identificado como uma causa raiz não solucionada.
- **REDE GOVERNO:** É uma rede de telecomunicação que permite a integração de diversos serviços, como voz, vídeo e dados, em uma estrutura única, formando a ideia de multisserviços. Foi instituído pelo Decreto Estadual nº 45.006/2009, visando a um melhor aproveitamento de recursos materiais, humanos, financeiros e orçamentários para a administração pública estadual.
- **SALAS DE TELECOM:** salas localizadas nas dependências da FAPEMIG que contém equipamentos de rede de dados a serem gerenciados/monitorados.

1.2.2. Projeto tecnológico da FAPEMIG

O licitante deverá observar a descrição do ambiente tecnológico apresentado a seguir para a proposição dos serviços licitados, levando-se em consideração todos os equipamentos existentes na atual Infraestrutura de TIC e as especificações dos equipamentos que irão compor a nova infraestrutura, considerando melhorias a serem realizadas e mudanças que por ventura possam ser solicitadas durante a execução do contrato.

1.2.2.1. Topologia da rede atual

O ambiente de redes da FAPEMIG utiliza tecnologia de Switching, permitindo a segmentação do ambiente de redes em diversas VLANs e o isolamento dos equipamentos Servidores em segmentos de alta velocidade, conforme Figura 1:

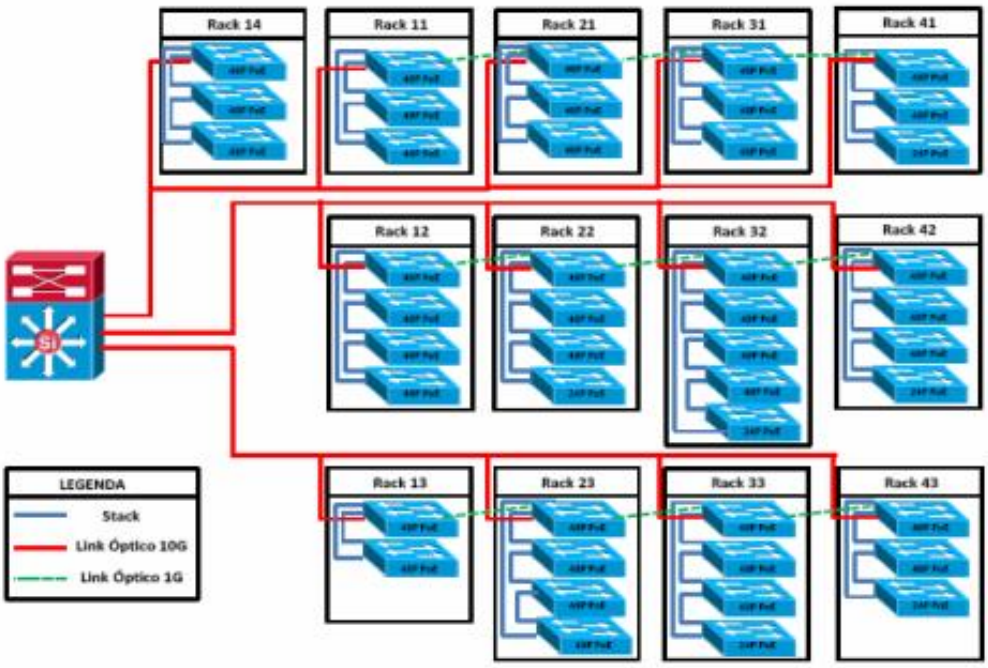

Figura 1: Topologia da rede atual

1.2.2.2. Elementos ativos da rede atual

Descrição dos elementos ativos que compõem a infraestrutura de rede local:

- **Switch Central:**

Switch Enterasys S8, com:

- 1 (um) módulo SK1208-0808-F6 - S-SERIES 1280GBPS LOAD SHARING - 8P 10GBASE-X ETHERNET SFP + 2 SLOT;
- 1 (um) switch Enterasys B5K125-48P2;
- 4 (quatro) fontes S-AC-OS.

- **Switches de Acesso #1 (Rack 11, Rack 21, Rack 31):**

Cada rack possui a seguinte composição de switches e acessórios:

- 1 (um) switch Enterasys B5K125-48P2
- 2 (dois) switches Enterasys B5G124-48P2
- 3 (três) cabos de empilhamento

- **Switches de Acesso #2 (Rack 41):**
  - 1 (um) switch Enterasys B5K125-48P2
  - 1 (um) switch Enterasys B5G124-48P2
  - 1 (um) switch Enterasys B5G124-24P2

- 3 (três) cabos de empilhamento

- **Switches de Acesso #3 (Rack 12, Rack 23):**

Cada rack possui a seguinte composição de switches e acessórios:

- 1 (um) switch Enterasys B5K125-48P2
- 3 (três) switches Enterasys B5G124-48P2
- 4 (quatro) cabos de empilhamento

- **Switches de Acesso #4 (Rack 22, Rack 42, Rack 33):**

Cada rack possui a seguinte composição de switches e acessórios:

- 1 (um) switch Enterasys B5K125-48P2
- 2 (dois) switches Enterasys B5G124-48P2
- 1 (um) switch Enterasys B5G124-24P2
- 4 (quatro) cabos de empilhamento

- **Switches de Acesso #5 (Rack 32):**

Cada rack possui a seguinte composição de switches e acessórios:

- 1 (um) switch Enterasys B5K125-48P2
- 3 (três) switches Enterasys B5G124-48P2
- 1 (um) switch Enterasys B5G124-24P2
- 5 (cinco) cabos de empilhamento

- **Switches de Acesso #6 (Rack 13):**
  - 1 (um) switch Enterasys B5K125-48P2
  - 1 (um) switch Enterasys B5G124-48P2
  - 2 (dois) cabos de empilhamento

- **Switches de Acesso #7 (Rack 43):**
  - 1 (um) switch Enterasys B5K125-48P2
  - 1 (um) switch Enterasys B5G124-48P2
  - 1 (um) switch Enterasys B5G124-24P2
  - 3 (três) cabos de empilhamento

- **Switches de Acesso #8 (Rack 14):**
  - 1 (um) switch Enterasys B5G124-48P2

- **Software de Gerenciamento:**
  - Enterasys NMS-BASE-50
  - Enterasys NAC-A-20 - NAC OUT-OF-BAND GATEWAY 3.000 ENDPOINTS OPTIONAL ON-BOARD ASSESSMENT

- **Controlador de rede sem fio #1**
  - 1 (uma) controladora Enterasys WS-C5210 - C5210 WLAN CONTROLLER. MANAGES 100 ACCESS POINTS EXPANDABLE

- **Ponto de Acesso Wireless**
  - 44 (quarenta e quatro) Enterasys WS-AP3710i – AP DUAL RADIO 3X3:3 MIMO INTEGRATED ANTENNA

1.2.2.3. Relação de equipamentos

Equipamento	Part #	Product Name	Product Description	Quantidade	End of Sale	End of Support
Módulo Fibra Ótica Switch S8	Enterasys SK1208-0808-F6	S-I/OFAB 8 SFP+ PORTS W2 OPSLOTS	S-I/OFAB 8 SFP+ PORTS W2 OPSLOTS	1	29/10/2014	31/12/2019
Switch de distribuição	Enterasys B5K125-48P2	B5 STK 48X3SPD+2SFPPLUS	B5 STK 48X3SPD+2SFPPLUS	13	30/06/2017	30/06/2022
Switch de acesso	Enterasys B5G124-48P2	B5 STK 48X3SPD-ATPOE+4SFP	B5 STK 48X3SPD-ATPOE+4SFP	25	30/06/2017	30/06/2022
Switch de acesso	Enterasys B5G124-24P2	B5 STK 24X3SPD-ATPOE+4SFP	B5 STK 24X3SPD-ATPOE+4SFP	6	30/06/2017	30/06/2022
Controladora Wireless	Enterasys WS-C5110-2-SR	C5110 WLAN controller	WS-C5210	1	31/12/2013	30/12/2018
Access Point	Enterasys WS-AP3710I	DUAL RADIO 3X3:3 MIMO INTEGRATED ANTENNA	DUAL RADIO 3X3:3 MIMO INTEGRATED ANTENNA	44	13/07/2015	31/07/2020

Tabela 2: Relação de equipamentos

1.2.2.4. Topologia e estruturação

A rede objeto desta especificação técnica deverá operar levando em conta os seguintes elementos:

- Cabeamento de fibra ótica na interligação dos andares e cabeamento UTP CAT 6 para atendimento aos usuários;

- Utilização de um "backbone" de alto desempenho (ethernet 10/40 Gbps), com mecanismos de contingência, e redundância completa, suportando evoluções futuras;
- Integração com a central trânsito de VoIP da Rede IP Multisserviços do Estado;
- Garantia de mobilidade dos usuários por todo o ambiente da FAPEMIG, permitindo que o usuário faça "logon" via rede wireless ou wired à sua rede de origem e tenha acesso aos seus serviços, independentemente de sua localização física;
- Segmentação da rede em VLANs por tipo de serviço (ex. voz, dados, vídeo) e por organizações e grupos de usuários;
- Utilização de QoS (Qualidade de Serviço) para priorização de tipo de serviço;
- Adoção de mecanismos de segurança e controle de acesso dos usuários e dispositivos conectados à rede;
- Utilização de no-breaks nas salas de telecomunicações do prédio, suportando todos os equipamentos da solução de rede de dados, garantindo a disponibilidade do serviço, em caso de falta de energia, por um período mínimo de 15 minutos;
- Utilização de no-break no Centro de Processamento de Dados – CPD (Data Center) do prédio, suportando todos os equipamentos e garantindo a disponibilidade do serviço, em caso de falta de energia, por um período mínimo de 15 minutos;
- Utilização de gerador no Centro de Processamento de Dados – CPD (Data Center) do prédio, suportando todos os equipamentos e garantindo a disponibilidade do serviço, em caso de falta de energia ou manutenção no gerador principal da FAPEMIG, por um período mínimo de 3 horas;
- A infraestrutura elétrica para utilização do gerador no Centro de Processamento de Dados – CPD (Data Center) do prédio será fornecida pela FAPEMIG;
- A potência dos equipamentos atuais do CPD é de aproximadamente 4.000 W e a tensão de fase da FAPEMIG é de 220 V e de linha de 380 V;
- Utilização de solução para monitoramento de temperatura e umidade do Centro de Processamento de Dados – CPD (Data Center), com envio de alertas.

1.2.2.5. Segurança de rede

Atualmente, todos os equipamentos de comunicação IP além dos computadores, tais como telefones IP, impressoras, Access Points, câmeras e outros, também são identificados e direcionados para suas respectivas VLANs de operação, evitando, com isso, possíveis ataques na rede de dados.

A rede está implementada de forma a garantir e preservar a mobilidade total dos usuários por todo o ambiente da FAPEMIG, permitindo que o usuário "log" à sua rede e tenha acesso aos seus serviços, independente da sua localização física, de maneira automática.

As novas soluções de segurança de rede devem contemplar serviços de valor agregado, bem como ativos de segurança de rede, serviços de criptografia de dados, serviços de monitoramento de atividade suspeita, resposta ao incidente, gestão de riscos e controle das políticas de segurança definidas para a FAPEMIG, e identificação e relatório de violações e atividades suspeitas.

A segurança de rede deverá ser composta dos seguintes elementos:

- Segregação da rede em redes lógicas virtuais através de VLANs e de VRF;
- Autenticação de Usuários: *Authentication, Authorization* e *Accounting* (Autenticação, Autorização e Registro), ou simplesmente AAA;
- NAC (*Network Access Control*) ou Controle de Acesso à Rede: O objetivo principal desta ferramenta é identificar o usuário/dispositivo no momento inicial de acesso à rede, permitindo apenas o acesso aos recursos a ele autorizados, possibilitando a gerência das informações e um controle de acesso mais efetivo;
- Next Generation Firewall-VPN;
- IPS (Intrusion Prevention System);
- Coleta de Logs de acesso;
- Correlacionador de eventos.

Deverão ser implementadas políticas de segurança para as estações de trabalho, por meio da verificação dos seguintes recursos:

- Verificação completa da imagem da estação de trabalho conectada e mobilização de rede de quarentena em caso de não conformidade;

- Servidor NAC: Responsável pela implementação das políticas de controle de acesso e pela integração com outros componentes da rede;
- Gerenciamento NAC: Responsável pela administração do NAC Server e armazenamento da base de dados dos usuários e regras de controle de acesso;
- Agente NAC: Cliente para solução NAC, independentemente do Sistema Operacional da estação de trabalho do usuário.

Deve ser implementado um Next Generation Firewall de alto desempenho na camada Core da rede.

O firewall de alto desempenho deverá fazer a segregação e proteção das redes de serviços compartilhados, onde estão instalados os servidores de autenticação, de arquivos e de monitoramento, bem como o controlador de chamadas, o controlador wireless e outros, permitindo acesso apenas aos recursos e serviços específicos. Os Switches Core e de Distribuição também têm um papel fundamental na solução de segurança de redes, possibilitando a configuração de listas de acesso de acordo com as necessidades do projeto.

Dispositivos IPS (Sistema de Prevenção de Intrusos) deverão ser instalados em pontos considerados estratégicos nos níveis de Distribuição-Core, para permitir a inspeção efetiva dos dados e a eficiência na mitigação de ameaças.

Dispositivos IPS também deverão ser utilizados nos perímetros dos equipamentos wireless (Access Points) devido à criticidade desta tecnologia.

A função principal do NAC é verificar se as estações de trabalho dos usuários estão em conformidade com a política de segurança definida pelos gestores de TIC da FAPEMIG. Caso não esteja, a estação terá acesso limitado à rede, podendo ingressar somente após o cumprimento das conformidades. Tão logo seja verificada a questão da conformidade das políticas de acesso, o NAC provisiona a aplicação do profile do usuário, de acordo com o seu grupo de mobilidade, na porta do switch onde ele fez logon, permitindo que o usuário utilize a sua rede (VRF/VLAN) e tenha acesso aos seus serviços, independente da sua localização física, dentro da estrutura da FAPEMIG.

A solução de segurança da rede deverá capturar todos os eventos e logs gerados pelos ativos de rede (switch, IPS, firewall etc.) e, por meio de correlação, identificar possíveis ataques, consolidando estas informações em uma interface gráfica. A

solução possibilita a customização do grau/criticidade dos ataques, facilitando a análise e mitigação pelo COS/Gestor.

1.2.2.6. Rede Wireless

Essa estrutura tem a função complementar a rede cabeada e suprir pelo menos as necessidades identificadas abaixo:

- Todos os Access Point trabalham no modo "Lightweight";
- Acesso à rede para notebooks e outros equipamentos de computação móvel, de usuários internos ou visitantes;
- Garantia de mobilidade aos usuários por todo o ambiente da FAPEMIG;
- Meio para integrar à solução de segurança de controle de acesso;
- Provisionamento de acesso para devices do tipo "tablet" para a rede de automação predial, proporcionando acesso aos dispositivos supervisórios das estruturas prediais;
- Suportar 400 usuários simultâneos;
- Garantia de entrega das mesmas funcionalidades presentes na rede cabeada.

O acesso por meio da rede wireless deverá ser disponibilizado em todas as áreas cobertas do subsolo, térreo, 1º, 2º e 3º andares do prédio da FAPEMIG.

Os novos APs (Access Points) deverão ser implementados nos padrões WiFi IEEE 802.11 a/b/g/n/ac (Wave-2).

O licitante deverá manter o quantitativo total atual de 44 (quarenta e quatro) APs do térreo, 1º, 2º e 3º andares, acrescidos de 6 (seis) APs para o subsolo.

Os Access Points serão alimentados por meio do cabeamento da rede ethernet (PoE – Power over Ethernet).

Vale ressaltar que a solução de controladores Wireless deverá possuir gerenciamento centralizado. A solução fornecida deverá controlar todos os APs da FAPEMIG obedecendo o requerimento de gerenciamento em ponto único centralizado.

Além dos Access Points definidos para acesso dos usuários, deverão ser provisionados equipamentos que funcionam em modo "*monitor mode*" (bloqueio, IDS etc.), fazendo

varredura das frequências de RF e gerando registros de logs e alertas quando são identificados quaisquer SSIDs não cadastrados na estrutura da FAPEMIG. Se os SSIDs encontrados não estiverem usando chaves de segurança, os APs que identificaram a ameaça tentam inviabilizar a ameaça através de DDoS (*Distributed Denial of Service*).

A solução de Rede Wireless deve ser capaz de:

- Localizar e rastrear clientes, dispositivos móveis e APs na planta;
- Ilustrar na planta da contratante a visualização de cobertura do ambiente de RF, bem como, a distribuição de canais;
- Permitir que o próprio usuário se cadastre na rede destinada a visitantes (*self registration*);
- Permitir captura de pacotes no ambiente Wi-Fi e integrar com analisador de pacotes Wireshark;
- Alertar sobre problemas de interferência de RF ou intermitência de conectividade existente no ambiente da contratante.

1.2.2.7. Rede Local (LAN)

Deverá ser mantida na rede física a sua segmentação em camada 2, através de implementação de VLANs (Virtual LAN), e em camada 3, através de VRFs (Virtual Routing and Forwarding), sendo adotados dois critérios de segregação: por organização/grupos de usuários e por tipo de serviço.

Na segmentação por serviço estão previstas as seguintes VLANs, de acordo com seus requisitos de qualidade de serviço:

- Dados;
- Voz;
- Monitoração;
- Autenticação e controle de acesso de usuários e dispositivos;
- Wireless;
- Visitantes;
- Automação Predial;

- Impressão.

A forma como a rede será segregada não deverá afetar a mobilidade dos usuários, garantindo que qualquer usuário se "log" em qualquer estação de trabalho conectada à rede e seja direcionado à sua VLAN e receba as permissões de acesso do seu perfil.

1.2.2.8. Camadas lógicas

A topologia da FAPEMIG é composta de três camadas lógicas com características, localização e funcionalidades específicas, conforme Figura 2:

Figura 2 – Camadas lógicas

Todo o cabeamento estruturado e de fibra ótica que atende ao projeto tecnológico da FAPEMIG, para Infraestrutura de TIC, está pronto e operacional, com exceção do cabeamento para os APs do subsolo e a redundância da fibra ótica na interligação entre salas de telecomunicações e Camada Core. Estes cabeamentos faltantes serão providenciados pela FAPEMIG.

Atualmente, cada sala de telecomunicação é interligada à Camada Core da rede por meio de fibra óptica, em conexões 10 Gigabit Ethernet. As salas de telecomunicações também se interligam entre si por meio de fibra óptica, em conexões 10 Gigabit Ethernet, sendo que cada sala de telecomunicação está conectada a pelo menos uma outra sala de telecomunicação.

Nos switches de distribuição localizados nas salas de telecomunicações são conectados os switches de acesso, utilizando fibras ópticas do tipo multímodo.

A partir dos switches de acesso, ocorre a distribuição da conexão dos pontos da rede local de computadores, telefones e demais dispositivos, utilizando o cabeamento estruturado UTP categoria 6 (das salas de telecomunicação até as tomadas localizadas no piso).

1.2.2.8.1. Camada Core

A Camada Core deverá ser composta por roteadores e switches nível (*layer*) 3 de alta capacidade, com a função de conectar os geradores de tráfego de dados aos pontos de abordagem das concessionárias e principais aplicações da rede da FAPEMIG.

Atualmente, a Camada Core possui apenas um switch. Entretanto, na substituição dos equipamentos, a Camada Core deverá ter switches redundantes e dimensionados para receber as conexões provenientes de todos os blocos e ainda se conectar aos links de comunicação com as concessionárias de voz e dados. Estes switches deverão ser interligados de forma a operar como uma única entidade lógica.

Na Camada Core, deverão ficar concentrados os serviços de balanceamento de carga (*Server Load Balancing*) e controladores da rede wireless, bem como, os elementos de segurança de rede: firewall, NAC, IPS, coleta de logs de acesso e correlacionador de eventos.

1.2.2.8.2. Camada de Distribuição e de Acesso

Os switches de distribuição deverão receber dois links redundantes da camada Core. Eles deverão estar corretamente dimensionados para receber as conexões provenientes de todos os andares.

Estes switches deverão ser interligados de forma a operar como uma única entidade lógica, agregando todo o tráfego proveniente das Salas de Telecom existentes nos andares através de 2 (dois) links de 10 Gigabit ethernet no modo ativo/ativo. Cada sala de Telecom deverá conter ao menos um switch de distribuição, nível (*layer*) 3.

A Camada Acesso deverá ser composta por switches dimensionados para conectar todos os pontos de usuários requeridos.

Deverá ser utilizada interface única para voz e dados, nos casos em que houver estação de trabalho e telefone IP juntos, e interface para voz e dados segregada, nos casos em que estes equipamentos estiverem instalados sozinhos. Os switches empregados deverão suportar dispositivos PoE. Toda a rede é composta de pontos de acesso gigabit ethernet, 1000BASE-T.

Os switches de distribuição e acesso são alocados em todas as salas de telecomunicações localizadas no subsolo, térreo, 1º, 2º e 3º andar do prédio, em razão da distribuição do cabeamento UTP CAT 6 nestas salas. Ou seja, cada uma das salas de Telecom atende a blocos específicos do andar, sendo necessário, portanto, que todas as salas sejam "ativas".

Cada switch de acesso está diretamente conectado aos switches de distribuição localizados nas salas de telecomunicação.

1.2.2.9. Volumetria de pontos de acesso e de equipamentos

Dos diversos dispositivos e equipamentos que acessam esta rede corporativa pode-se citar: computadores, notebooks, câmeras de vigilância, leitores biométricos, Access Points, aparelhos telefônicos, entre outros.

1.2.2.9.1. Switches e pontos de acesso físico

É esperado na licitação o fornecimento, pela CONTRATADA, de 2 (dois) Switches Core (redundantes), pelo menos um Switch de Distribuição por sala de telecomunicação e Switches Acesso, observando as especificações técnicas do Anexo III – ESPECIFICAÇÕES DOS ATIVOS DE REDE, para atender a seguinte quantidade de pontos de acesso físico:

FAPEMIG		
Andar	**Localização**	**Portas de Switch (Dados+Voz+Periféricos)**
Subsolo	Sala de Telecom	48
Térreo	Sala de Telecom 3	48
	Sala de Telecom 2	144
	Sala de Telecom 1	96
1º andar	Sala de Telecom 3	144
	Sala de Telecom 2	168

	Sala de Telecom 1	96
2º andar	Sala de Telecom 3	120
	Sala de Telecom 2	192
	Sala de Telecom 1	72
3º andar	Sala de Telecom 3	72
	Sala de Telecom 2	120
	Sala de Telecom 1	120
Total		1440

Tabela 3 – Portas de Switch por localização

1.2.2.9.2. Pontos de acesso wireless

O acesso através da rede wireless deverá ser disponibilizado em todas as áreas cobertas do subsolo, térreo, 1º, 2º e 3º andares do prédio da FAPEMIG com garantia de mobilidade aos usuários por todo o ambiente da FAPEMIG.

Para o subsolo, térreo, 1º, 2º e 3º andares, a quantidade esperada de Access Points – APs é de 50 (cinquenta) APs, observando as especificações técnicas do Anexo III – ESPECIFICAÇÕES DOS ATIVOS DE REDE.

1.2.2.9.3. Outros equipamentos

Item	Quantidade mínima esperada
Next Generation Firewall	1
Servidor NAC	1
Gerente NAC	1
Controlador e/ou Gerência dos controladores wireless	1

Tabela 4 – Quantidade mínima esperada por equipamento

Caso o licitante ofereça equipamentos com dois ou mais itens listados acima de maneira integrada em um único equipamento, o quantitativo deve ser ajustado de forma a considerar esta integração. É imprescindível que todos os itens da Tabela 4 estejam presentes na solução ofertada, observando as especificações técnicas do Anexo III – ESPECIFICAÇÕES DOS ATIVOS DE REDE.

1.2.3. Cronograma e implantação

A implantação dos serviços de infraestrutura de rede de dados, objeto desta contratação, ocorrerá com entregas modulares e progressivas, compatíveis com o *End of Support*, fim do ciclo de vida dos equipamentos operantes atualmente na FAPEMIG.

1.2.3.1. Cronograma de ativação da solução

Item	Prazo para ativação
Next Generation Firewall	60 dias após o início da vigência do contrato
Switches Core	60 dias após o início da vigência do contrato
Servidor NAC	90 dias após o início da vigência do contrato
Gerente NAC	90 dias após o início da vigência do contrato
Controlador e/ou Gerência dos controladores wireless	90 dias após o início da vigência do contrato
Access Points - APs	90 dias após o início da vigência do contrato
Switches de Distribuição e Acesso	180 dias após o início da vigência do contrato

Tabela 5 – Cronograma de ativação da solução

A Tabela 5 apresenta todo o plano de demanda para a solução contratada e que deverá ser considerada para a elaboração da proposta.

A CONTRATADA assume a operação, atualização das soluções, gerenciamento, monitoramento, suporte técnico, manutenção preventiva e manutenção corretiva de todos os equipamentos atuais de infraestrutura de rede de dados da FAPEMIG desde o início da vigência do contrato até a ativação da solução que substituirá os equipamentos atuais. Os equipamentos atuais de infraestrutura de rede de dados deverão ser considerados na elaboração da proposta comercial.

Em caso de necessidade de substituição de equipamentos da rede atual da FAPEMIG antes do prazo de ativação, para garantia da disponibilidade do serviço, a

CONTRATADA deverá implantar as soluções e equipamentos que compõe a proposta comercial da CONTRATADA

1.2.4. Transição dos serviços

I. Os primeiros 60 (sessenta) dias corridos após o início da vigência do contrato são considerados como período de transição, durante o qual a CONTRATADA deverá efetuar todas as atividades necessárias para assumir inteiramente a prestação dos serviços a serem contratados, constantes neste Termo de Referência.

II. Durante o período de transição, a CONTRATADA deverá:

   a. Efetuar reuniões e consultoria junto a CONTRATANTE de forma a possibilitar o estabelecimento formal dos fluxos de trabalhos e dos processos necessários para a implementação dos serviços a serem contratados, constantes neste termo de referência;

   b. Documentar e solicitar aceite da CONTRATANTE de todos os procedimentos executados durante o período de transição e apresentá-los a cada 15 (quinze) dias corridos à CONTRATANTE de forma a comprovar a execução dos serviços realizados;

   c. Apresentar quinzenalmente ao Gestor do Contrato relatórios gerenciais de status para acompanhamento detalhando: atividades realizadas, atrasos em atividades e suas causas, problemas identificados, riscos identificados, entre outras;

   d. Avaliar toda documentação a ser disponibilizada pela CONTRATANTE referente à Infraestrutura de TIC;

   e. Instalar, configurar, testar e homologar todos os softwares e hardwares para garantir a operação, gerenciamento e monitoramento de toda a Infraestrutura de TIC da CONTRATANTE;

   f. Conhecer todos os processos de atendimento da central de Service Desk da CONTRATANTE;

   g. Visitar e inspecionar todos os equipamentos instalados nas salas de telecom e data center da FAPEMIG;

   h. Realizar todas as atividades necessárias para garantir o início da operação após o período de transição.

III. As eventuais perdas de SLA que ocorrerem durante o período de transição não serão consideradas para efeito de ajuste no pagamento.

IV. Após o período de transição inicia-se a medição dos indicadores. Os primeiros 30 (trinta) dias corridos após o período de transição dos serviços serão considerados como período de ajustes específicos, durante o qual as metas definidas podem ser flexibilizadas por acordo das partes. As eventuais perdas de SLA que ocorrerem neste período não serão consideradas para efeito de ajuste no pagamento.

V. A CONTRATADA assume desde o início da vigência do contrato, inclusive no período de transição dos serviços, a operação, a atualização das soluções, o gerenciamento, o monitoramento, o suporte técnico, a manutenção preventiva e a manutenção corretiva de todos os equipamentos atuais de infraestrutura de rede de dados da FAPEMIG.

VI. Em caso de necessidade de substituição de equipamentos da rede atual da FAPEMIG antes do prazo previsto de ativação, inclusive no período de transição dos serviços, a CONTRATADA deverá implantar as soluções e equipamentos que compõe a proposta comercial da CONTRATADA para garantia da disponibilidade do serviço.

1.2.5. Organização funcional dos fornecedores de serviços de TIC da FAPEMIG

A Central de Serviços (Service Desk) de atendimento e suporte aos usuários TIC da FAPEMIG tem o papel de agente centralizador das ações e interações com os prestadores de serviço de TIC. A Central de Serviços é o ponto de contato entre os usuários de TIC e os diversos fornecedores das soluções de tecnologia para a FAPEMIG. Além de fazer a interface entre usuários e demais fornecedores, a Central de Serviços tem a função de gerenciar as solicitações e chamados, tratando-as em um dos três níveis existentes e registrando a sua abertura, progresso e fechamento (condicionado à solução do problema), registrando ainda todas as informações referentes ao atendimento efetuado.

Desta forma, o fornecedor dos serviços de infraestrutura de rede deverá estabelecer uma interface de comunicação e de troca de informações direta com o Service Desk, alinhando eventuais intervenções, indisponibilidades e quaisquer atividades que afetem os usuários de TIC.

Os serviços de Service Desk não fazem parte do escopo deste edital, sendo prestados por empresa específica contratada com essa finalidade, cabendo à CONTRATADA a resolução dos incidentes da Infraestrutura de TIC.

1.2.6. Requerimento de desempenho

1.2.6.1. Classificação dos serviços

Ficam definidos três níveis de prioridade para fins de atendimento e resolução dos chamados e solicitações dos usuários, de acordo com o cargo do autor do chamado e com o tipo do motivo do chamado, sendo eles:

- Prioridade 1: O problema impede o trabalho do usuário, ou grupo de usuários, ou é um chamado do grupo prioritário;

- Prioridade 2: O problema afeta a produtividade do trabalho do usuário/grupo (interrupção parcial de funções, mau funcionamento de recursos, intermitência);

- Prioridade 3: O chamado é relacionado a melhorias, customizações e demais alterações sem impacto no trabalho e produtividade do usuário/grupo (instalação de softwares, mudanças físicas de equipamentos, configurações e demais customizações necessárias).

Entende-se como usuário a pessoa ou grupo de pessoas solicitante e usuária do ambiente de tecnologia da FAPEMIG.

Farão parte do grupo prioritário os chamados provenientes da Presidência, Chefe de Gabinete, Assessor(a) Especial da Presidência, Procurador(a) Chefe, Chefe da Unidade Seccional de Controle Interno, Diretor(a) de Ciência, Tecnologia e Inovação, Diretor(a) de Planejamento, Gestão e Finanças, Coordenador(a) Científica e de Inovação e Coordenador(a) Geral de Gestão. Estima-se que o total de usuários pertencentes ao grupo prioritário é igual a 13 (treze).

1.2.6.2. Atendimento e indicadores de desempenho

A CONTRATADA deverá garantir total disponibilidade e qualidade de toda a Infraestrutura de TIC, além de atender as solicitações dos usuários, prestação de assistência técnica e suporte em conformidade com a Tabela 6. Entende-se como qualidade da infraestrutura, o respeito às especificações exigidas, tanto em termos

de funcionalidades requeridas, quanto em termos de latência, capacidade de tráfego e demais itens especificados no edital e seus anexos.

Tabela 6 - Prazos máximos de atendimento e solução

Prazos Máximos de Atendimento e Solução								
Atendimento	**Atendimento 07h00min às 19h00min, dias úteis**						**Atendimento 19h01min às 06h59min, dias úteis, sábados, domingos e feriados**	
Serviço	**Prioridade 1**		**Prioridade 2**		**Prioridade 3**		**Plantão**	
	Atendimento	**Solução**	**Atendimento**	**Solução**	**Atendimento**	**Solução**	**Atendimento**	**Solução**
Solicitações realizadas ao COR+COS	10 min	2 h	20 min	4 h	20 min	8 h	30 min	8 h

Para interpretação da Tabela 6, entende-se por atendimento o intervalo de tempo entre o momento em que o chamado é direcionado para a fila de atendimento da CONTRATADA e o momento em que o analista responsável assume o atendimento do incidente. Entende-se por solução o tempo gasto pelo analista para solucionar o incidente depois de assumi-lo.

A CONTRATADA deverá manter a disponibilidade de todos os equipamentos que compõe a infraestrutura da de Rede da FAPEMIG com um Índice de Disponibilidade do Ambiente de 99,90% (noventa e nove vírgula noventa por cento) no horário comercial e de 98,50% (noventa e oito vírgula cinquenta por cento) no horário de plantão, apurados mensalmente, conforme descrito nas tabelas abaixo:

INDICADOR: INCIDENTES ATENDIDOS NO PRAZO – M1	
Índice de Incidentes Atendidos no Prazo (IAP), conforme Tabela 6.	
Item	**Descrição**
Finalidade	Reduzir os atrasos nos atendimentos dos incidentes registrados nas filas **CONTRATADA**
Meta exigida	>=95,00% (noventa e cinco por cento)
Instrumento de Medição	Relatório mensal extraído da ferramenta de Service Desk, consolidado e emitido pela **CONTRATADA**
Periodicidade	Aferição mensal após encerramento do período de apuração

Fórmula de cálculo	**IAP = (TIA / TIR) x 100, onde** **TIA** = Total de Incidentes Atendidos dentro do prazo **TIR** = Total de Incidentes Registrados durante o período de apuração
Faixa de Ajuste no pagamento (M1)	Se **IAP** >= 95,00 (inclusive) **M1**= 1,0 Se **IAP** entre 95,00 e 90,00 (inclusive), **M1**= 0,9 Se **IAP** entre 90,00 e 85,00 (inclusive), **M1**= 0,8 Se **IAP** entre 85,00 e 80,00 (inclusive), **M1**= 0,7 Se **IAP** entre 80,00 e 75,00 (inclusive), **M1**= 0,6 Se **IAP** abaixo de 75,00, **M1**= 0,5
Sanções	Se **IAP** abaixo de 75,00 por 3 (três) meses consecutivos, será considerada inexecução parcial do ajuste e a **CONTRATANTE** poderá rescindir o contrato. O não atingimento da meta implicará em desconto no valor do pagamento mensal, do serviço correspondente ou da garantia contratual especificada neste instrumento. O desconto total será calculado aplicando cumulativamente o desconto referente a cada indicador de qualidade especificado nesta tabela e aplicável no período de apuração correspondente.
Início da vigência	Após 60 (sessenta) dias corridos da data de início da vigência do contrato.
Observações	Este indicador é cumulativo com os indicadores M2, M3, M4 e M5

Tabela 7 - Incidentes atendidos no prazo – M1

INDICADOR: INCIDENTES SOLUCIONADOS NO PRAZO – M2	
Índice de Incidentes Solucionados no Prazo (ISP), conforme Tabela 6.	
Item	**Descrição**
Finalidade	Reduzir os atrasos na solução dos incidentes registrados nas filas de atendimento da **CONTRATADA**
Meta exigida	>= 95,00% (noventa e cinco por cento)
Instrumento de Medição	Relatório mensal extraído da ferramenta de Service Desk, consolidado e emitido pela **CONTRATADA**
Periodicidade	Aferição mensal após encerramento do período de apuração
Fórmula de cálculo	**ISP = (TCS / TCA) x 100**, **onde:** **TCS** = Total de Chamados Solucionados dentro do prazo máximo definido neste instrumento, durante o período de apuração. **TCA** = Total de Chamados Abertos durante o período de apuração.

Faixa de Ajuste no pagamento (M2)	Se **ISP** >=95,00 (inclusive), **M2** = 1,0 Se **ISP** entre 95,00 e 90,00 (inclusive), **M2** = 0,9 Se **ISP** entre 90,00 e 85,00 (inclusive), **M2** = 0,8 Se **ISP** entre 85,00e 80,00 (inclusive), **M2** = 0,7 Se **ISP** entre 80,00 e 75,00 (inclusive), **M2** = 0,6 Se **ISP** abaixo de 75,00, **M2** = 0,5
Sanções	Se **ISP** abaixo de 75,00 por 3 (três) meses consecutivos, será considerada inexecução parcial do ajuste e a **CONTRATANTE** poderá rescindir o contrato. O não atingimento da meta implicará em desconto no valor do pagamento mensal, do serviço correspondente ou da garantia contratual especificada neste instrumento. O desconto total será calculado aplicando cumulativamente o desconto referente a cada indicador de qualidade especificado nesta tabela e aplicável no período de apuração correspondente.
Início da vigência	Após 60 (sessenta) dias corridos da data de início da vigência do contrato.
Observações	Este indicador é cumulativo com os indicadores M1, M3, M4 e M5

Tabela 8 - Chamados solucionados no prazo – M2

INDICADOR: DISPONIBILIDADE MENSAL DA INFRAESTRUTURADE TIC EM HORARIO COMERCIAL – M3	
Percentual de tempo em que todos os equipamentos que compõem a Infraestrutura de TIC, permaneceram em condições normais de funcionamento, durante o horário comercial	
Item	**Descrição**
Finalidade	Minimizar o tempo de indisponibilidade dos equipamentos no horário comercial
Meta exigida	>= 99,90% (noventa e nove, noventa por cento)
Instrumento de Medição	Relatório mensal extraído da ferramenta de monitoramento e gerenciamento da **Infraestrutura de TIC**, consolidado e emitido pela **CONTRATADA**
Periodicidade	Aferição mensal apurada após encerramento do período de apuração

Fórmula de cálculo	**IDIC = (Σ(TDEC) / (NEQ × NHC)) × 100** **onde:** **IDIC =** Índice de Disponibilidade Mensal da Infraestrutura de TIC no horário comercial **Σ(TDEC)** = Somatório do Tempo de Disponibilidade de cada Equipamento no mês durante o horário comercial (em horas) **NEQ**= Número de Equipamentos **NHC** = Número de Horas no mês, em horário comercial
Faixa de Ajuste no pagamento (M3)	Se **IDIC** >= 99,90 (inclusive), **M3** = 1,0 Se **IDIC** entre 99,90 e 98,00 (inclusive), **M3** = 0,9 Se **IDIC** entre 98,00 e 96,00 (inclusive), **M3** = 0,8 Se **IDIC** entre 96,00 e 94,00 (inclusive), **M3** = 0,7 Se **IDIC** entre 94,00 e 92,00 (inclusive), **M3** = 0,6 Se **IDIC** abaixo de 92,00, **M3** = 0,5
Sanções	Se **IDIC** abaixo de 92,00 por 3 (três) meses consecutivos, será considerada inexecução parcial do ajuste e a **CONTRATANTE** poderá rescindir o contrato. O não atingimento da meta implicará em desconto no valor do pagamento mensal, do serviço correspondente ou da garantia contratual especificada neste instrumento. O desconto total será calculado aplicando cumulativamente o desconto referente a cada indicador de qualidade especificado nesta tabela e aplicável no período de apuração correspondente.
Início da vigência	Após 60 (sessenta) dias corridos da data de início da vigência do contrato
Observações	Este indicador é cumulativo com os indicadores M1, M2, M4 e M5

Tabela 9 - Disponibilidade mensal da solução em horário comercial – M3

INDICADOR: DISPONIBILIDADE MENSAL DA INFRAESTRUTURA DE TIC EM HORÁRIO DE PLANTÃO - M4	
Percentual de tempo em que todos os equipamentos que compõe a Infraestrutura de TIC, permaneceram em condições normais de funcionamento, durante o horário de plantão.	
Item	**Descrição**
Finalidade	Minimizar o tempo de indisponibilidade dos equipamentos no horário de plantão
Meta exigida	>= 98,50% (noventa e oito, cinquenta por cento)

Instrumento de Medição	Relatório mensal extraído da ferramenta de monitoramento e gerenciamento da Infraestrutura de TIC, consolidado e emitido pela **CONTRATADA**
Periodicidade	Aferição mensal apurada após encerramento do período de apuração
Fórmula de cálculo	**IDIP= (Σ(TDEP) / (NEQ × NHP)) × 100** **onde:** **IDIP =** Índice de Disponibilidade Mensal da Infraestrutura de TIC no horário de plantão **Σ(TDEP)** = Somatório do Tempo de Disponibilidade de cada Equipamento no mês no horário de plantão (em horas) **NEQ**= Número de Equipamentos **NHP** = Número de Horas no mês, em horário de plantão
Faixa de Ajuste no pagamento (M4) - PAREI	Se **IDIP** >= a 98,50 (inclusive), **M4** = 1,0 Se **IDIP** entre 98,50 e 96,50 (inclusive), **M4** = 0,9 Se **IDIP** entre 96,50 e 94,50 (inclusive), **M4** = 0,8 Se **IDIP** entre 94,50 e 92,50 (inclusive), **M4** = 0,7 Se **IDIP** entre 92,50 e 90,00 (inclusive), **M4** = 0,6 Se **IDIP** abaixo de 90,00, **M4** = 0,5
Sanções	Se **IDIP** abaixo de 90,00 por 3 (três) meses consecutivos, será considerada inexecução parcial do ajuste e a **CONTRATANTE** poderá rescindir o contrato. O não atingimento da meta implicará em desconto no valor do pagamento mensal, do serviço correspondente ou da garantia contratual especificada neste instrumento. O desconto total será calculado aplicando cumulativamente o desconto referente a cada indicador de qualidade especificado nesta tabela e aplicável no período de apuração correspondente.
Início da vigência	Após 60 (sessenta) dias corridos da data de início da vigência do contrato.
Observações	Este indicador é cumulativo com os indicadores M1, M2, M3 e M5

Tabela 10 - Disponibilidade mensal da solução em horário de plantão - M4

INDICADOR: RECLAMAÇÕES DE ATENDIMENTO - M5	
Índice de reclamações de atendimento (IREC)	
Item	**Descrição**
Finalidade	Avaliar o percentual de reclamação referentes aos atendimentos realizados pela CONTRATADA, garantindo que os atendimentos sejam realizados com qualidade e com o menor percentual de reclamações
Meta exigida	<= 3% (três por cento)
Instrumento de Medição	Relatório mensal extraído da ferramenta de Service Desk, de acordo com o resultado mensal da pesquisa de satisfação.
Periodicidade	Aferição mensal apurada após o fechamento dos chamados abertos nos grupos de solução criados para a CONTRATADA
Fórmula de cálculo	**IREC = (TRA / TAR) x 100**, Onde: **TRA** = Total de reclamações de atendimento **TAR** = Total de chamados atendidos no período de medição
Faixa de Ajuste no pagamento (M5)	Se **IREC** menor ou igual a 3,00, **M5** = 1,0 Se **IREC** entre 3,00 e 4,00 (inclusive), **M5** = 0,9 Se **IREC** entre 4,00 e 5,0 (inclusive), **M5** = 0,8 Se **IREC** entre 5,00 e 6,00 (inclusive), **M5** = 0,7 Se **IREC** entre 6,00 e 7,00 (inclusive), **M5** = 0,6 Se **IREC** acima de 7,00, **M5** = 0,5
Sanções	Se **IREC** acima de 7,00 por 3 (três) meses consecutivos, será considerada inexecução parcial do ajuste e a **CONTRATANTE** poderá rescindir o contrato. O não atingimento da meta implicará em desconto no valor do pagamento mensal, do serviço correspondente ou da garantia contratual especificada neste instrumento. O desconto total será calculado aplicando cumulativamente o desconto referente a cada indicador de qualidade especificado nesta tabela e aplicável no período de apuração correspondente.
Início da vigência	Após 60 (sessenta) dias corridos da data de início da vigência do contrato.
Observações	Este indicador é cumulativo com os indicadores M1, M2, M3 e M4

Tabela 11 - Reclamações de atendimento - M5

1.2.6.3. Da disponibilidade da infraestrutura

I. Para medir a disponibilidade da infraestrutura, a CONTRATADA deverá disponibilizar uma solução de monitoramento e gerenciamento que deverá

possuir, no mínimo, as funcionalidades descritas no Anexo II – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE MONITORAMENTO E GERENCIAMENTO.

II. A CONTRATADA deverá fornecer toda a infraestrutura necessária (hardware, software, conexão de dados etc.) para o funcionamento da solução de monitoramento e gerenciamento, instalar, configurar e cadastrar todos os ativos a serem monitorados e solicitar a sua homologação junto à CONTRATANTE, em até 60 (sessenta) dias após o início da vigência do contrato.

III. Serão objetos de monitoração para medição de disponibilidade todos os equipamentos constantes no ANEXO III – ESPECIFICAÇÕES DOS ATIVOS DE REDE e que estejam com status ATIVO no CMDB e todos os equipamentos da infraestrutura atual que também estejam com status ATIVO no CMDB.

IV. Para efeito de comprovação da disponibilidade só serão aceitos os relatórios gerados pela solução de monitoramento e gerenciamento. Dessa forma, o(s) período(s) em que a solução de monitoramento estiver indisponível ou quando o equipamento não estiver sendo monitorado por qualquer motivo, com exceção dos previstos no item 1.2.6.3.IX, serão considerados como indisponibilidade.

V. A CONTRATADA poderá optar por manter a solução de monitoramento e gerenciamento instalada nas suas dependências ou nas dependências da CONTRATANTE, ou, se preferir, nos dois ambientes. Dessa forma, o monitoramento poderá ser feito local ou remotamente.

VI. A CONTRATADA deverá entregar, mensalmente, à CONTRATANTE o relatório de disponibilidade dos equipamentos, considerando os horários comercial e de plantão.

VII. A CONTRATADA deverá liberar acesso completo a partir das estações de trabalho da CONTRATANTE (até 03 acessos simultâneos) a qualquer solução de monitoramento, gerenciamento, funcionalidades de auditoria, consulta, criação e geração de relatórios.

VIII. Caso seja necessário, a CONTRATANTE poderá solicitar acesso a qualquer outra funcionalidade da solução que deverá ser acessada com o acompanhamento de técnicos da CONTRATADA. O acesso deverá ser agendado e solicitado com antecedência mínima de 24 (vinte e quatro) horas corridas.

IX. As paradas programadas para ajustes e atualização de qualquer item da infraestrutura, desde que previamente autorizadas pela CONTRATANTE, bem como as perdas de monitoramento em função de problemas de responsabilidade da CONTRATANTE, não serão consideradas como indisponibilidade para efeito de faturamento.

1.2.7. Assistência técnica

I. A CONTRATADA deverá prestar serviços de assistência técnica e de manutenção corretiva e preventiva a todos os equipamentos e softwares da infraestrutura de rede de dados da FAPEMIG, tanto dos equipamentos que compõe a rede atual, quanto dos novos equipamentos que vierem a ser instalados ou substituídos, com atualização de softwares, substituição de equipamentos defeituosos, troca de peças e partes defeituosas, caso necessário, durante todo o período de vigência do contrato, obedecendo ao Regime de Operação, Classificação dos Serviços e os Requerimentos de Desempenho, estabelecidos os Itens 8.2.IV, 1.2.6.1 e 1.2.6.2 e com as condições descritas neste Termo de Referência.

   a. A CONTRATADA deverá manter, durante todo o período de vigência do contrato, todos os softwares devidamente atualizados, o que o inclui: atualização de versão, aplicação de patches, correções, hot fix e service packs etc.

II. A CONTRATADA deverá apresentar declaração de acordo com o modelo do ANEXO IV – DECLARAÇÃO DE GARANTIA DE ASSISTÊNCIA TÉCNICA, garantindo que, durante todo o período de vigência do contrato, a assistência técnica, a manutenção corretiva e evolutiva de todos os equipamentos e softwares, bem como os que vierem a ser incorporados à infraestrutura da rede FAPEMIG, serão de sua inteira responsabilidade, devendo arcar com todos os seus custos, inclusive os decorrentes de intervenções por parte dos fabricantes dos equipamentos. Para os equipamentos da rede atual, a COTRATADA garantirá a assistência técnica, manutenção corretiva e evolutiva, desde o início da vigência do contrato, para aqueles equipamentos que forem mantidos na infraestrutura de rede da FAPEMIG, observando os prazos de ativação das soluções estabelecidos no item 1.2.3.1.

III. A prestação de serviços técnicos de assistência técnica e de manutenção corretiva e preventiva deverá compreender:

   a. Prestação de serviços de manutenção corretiva no local de instalação dos equipamentos;

b. Fornecimento e instalação de atualizações corretivas e evolutivas (upgrade de versões) de softwares, necessários ao perfeito funcionamento dos equipamentos descritos, por intermédio de técnico presente *on site*;

c. Qualquer software, atualização ou upgrade de software, que venha a ser instalado, deverá estar devidamente licenciado, ser original do fabricante e de qualidade e características técnicas iguais ou superiores às existentes no equipamento, bem como deve ser compatível com este, devendo ser configurado de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades de alta disponibilidade e redundância operacionais. A CONTRATANTE poderá rejeitar a instalação de software, a atualização ou o upgrade de software que não atenda a estas características;

d. Substituição de módulos, componentes, peças e materiais defeituosos, mesmo que tais defeitos não tenham causado interrupção da rede. Os módulos, componentes, peças e materiais utilizados em substituição aos defeituosos, deverão ser novos, de primeiro uso, originais do fabricante e de qualidade e características técnicas iguais ou superiores às existentes no equipamento, bem como devem ser compatíveis com este.

IV. Todo o procedimento de fornecimento, instalação, configuração e operação na FAPEMIG será acompanhado e validado pela CONTRATANTE.

V. Todos os softwares e equipamentos fornecidos pela CONTRATADA para substituir softwares e equipamentos em função de defeito serão fornecidos sem ônus para a CONTRATANTE e incorporados ao patrimônio da CONTRATANTE.

VI. Todos os equipamentos da CONTRATANTE que vierem a ser substituídos em função de defeito deverão ser entregues à CONTRATADA que providenciará a sua baixa no CMDB e seu recolhimento, sem ônus para a CONTRATANTE.

VII. Todos os ativos fornecidos para a execução dos serviços contratados serão verificados quanto ao cumprimento das especificações e funcionalidades requeridas no edital e seus anexos.

VIII. Todas as solicitações de serviços de assistência técnica e de manutenção corretiva e preventiva deverão ser registradas por chamado pela CONTRATADA, em software disponibilizado pela CONTRATANTE. A abertura dos chamados poderá ser efetuada por website ou Central de Serviços,

contendo no mínimo as seguintes informações: Data e hora da solicitação; Descrição da ocorrência; Número do registro/ocorrência; Identificação do solicitante; Identificação do atendente; Prioridade da ocorrência. A CONTRATADA deverá registrar no software disponibilizado pela CONTRATANTE todas as etapas das manutenções corretivas e preventivas.

IX. Os serviços de assistência técnica e de manutenção corretiva e preventiva dos equipamentos e softwares descritos no Item 1.2.2.2 (Elementos ativos da rede atual) e os novos equipamentos que vierem a ser instalados ou substituídos, deverão obedecer, durante todo o período de vigência do contrato, os critérios abaixo, considerando a camada que cada um pertence.

X. No caso de defeito dos equipamentos, a CONTRATADA deverá solucionar o problema de acordo com os prazos estabelecidos na Tabela 12:

Camada	Período de abertura de chamado	Prazos Máximos para Identificação da Causa do Problema (horas corridas)	Prazos Máximos para Reparo (horas úteis)
Core	24 x 7 x 365	2	4
Distribuição	24 x 7 x 365	2	6
Acesso	24 x 7 x 365	2	8

Tabela 12 - Prazos de identificação do problema e reparo

a. Caso o defeito não tenha sido identificado e/ou solucionado ou o equipamento não tenha sido substituído dentro dos prazos máximos especificados na Tabela 12 os tempos excedentes serão considerados como indisponibilidade.

b. Prazo Máximo para Identificação da Causa do Problema: Tempo decorrido entre a abertura do chamado pela CONTRATANTE ou pela CONTRATADA, e o momento em que a CONTRATANTE assume o chamado com a identificação do hardware (módulos, componentes, peças ou materiais) e/ou softwares responsáveis pelo mau funcionamento de equipamento.

c. Prazo Máximo para Reparo: Tempo decorrido entre a identificação do problema e a substituição ou reparo do hardware (módulos, componentes, peças e materiais defeituosos) e/ou atualização de software ou aplicação de patches e correções, de forma a garantir a colocação do equipamento em plenas condições de funcionamento.

d. Caso seja necessário substituir outros equipamentos e/ou softwares para garantir a compatibilidade com a solução já implantada na FAPEMIG, a CONTRATADA deverá fornecer e implantar as soluções e equipamentos que compõe a proposta comercial da CONTRATADA para garantia da disponibilidade do serviço, sem ônus para a CONTRATANTE.

XI. Para os itens a serem fornecidos pela CONTRATADA em substituição aos equipamentos e softwares da rede atual de acordo com o cronograma de ativação das soluções, deverão ser observados os seguintes critérios e procedimentos:

a. Todos os equipamentos e softwares que serão fornecidos para substituição da infraestrutura atual da FAPEMIG deverão possuir garantia e assistência técnica do próprio fabricante, durante todo o período de vigência do contrato, fornecida pelo fabricante ou por parceiro autorizado.

i. Os serviços de garantia e assistência técnica deverão possibilitar o acesso remoto do fabricante aos equipamentos para ajudar na correção de problemas dos diversos tipos, inclusive configuração, sem custos adicionais para a CONTRATANTE;

b. A CONTRATADA deverá comprovar essa garantia, por meio de declaração expedida pelo fabricante, até a data prevista para ativação da solução.

c. Em caso de defeito e esgotadas todas as possibilidades de conserto pelo fabricante, os equipamentos deverão ser substituídos por equipamentos novos, de características técnicas e desempenho igual ou superior ao equipamento original, do mesmo fabricante e com ciclo de vida ativo, conforme indicação de modelo do fabricante e que garanta toda a compatibilidade com toda a solução instalada.

d. Para os itens da rede atual da FAPEMIG, enquanto não forem substituídos pela CONTRATANTE de acordo com o cronograma de ativação das soluções, deverão ser observados os seguintes critérios e procedimentos:

i. Em caso de defeito e esgotadas todas as possibilidades de conserto, a CONTRATADA deverá implantar as soluções e equipamentos que compõe a proposta comercial da CONTRATADA para garantia da disponibilidade do serviço.

ii. A CONTRATADA poderá disponibilizar equipamentos reserva (*spare*) do mesmo fabricante, mesmo modelo ou superior ao equipamento defeituoso, por um prazo máximo de 90 (noventa) dias corridos, desde que garantida a compatibilidade com o ambiente. Findo o prazo de 90 (noventa) dias corridos, será considerado como indisponibilidade, mesmo que o equipamento esteja em funcionamento, até que seja substituído por outro equipamento nas condições definidas no subitem 1.2.7.XI.d.i.

1.2.8. Manutenção e Assistência técnica do cabeamento lógico estruturado

A CONTRATADA é responsável pelo fornecimento, manutenção e organização de todos os *patch panels* e *patch cords* do cabeamento UTP CAT 6, provendo as conexões entre os switches de acesso e os *patch panels*, e cordões ópticos em todos os racks das salas de Telecom e do Data Center da FAPEMIG.

1.2.9. Das alterações na infraestrutura de TIC

Durante o período de vigência do contrato, de acordo com as necessidades da CONTRATANTE, poderão ocorrer modificações no projeto para melhor adequação técnica à execução dos serviços. É de responsabilidade da CONTRATADA documentar todas as alterações que venham a acontecer na infraestrutura, principalmente no que diz respeito à inclusão de novos itens. A CONTRATADA será responsável pela atualização de toda a documentação da topologia de rede e dos demais documentos gerados nas eventuais mudanças.

As alterações de especificações, elaboração/atualização de documentação, bem como configuração e integração dos novos itens de configuração (hardware e software) que vierem a integrar a Infraestrutura de TIC, deverão ser realizadas pela CONTRATADA sem custo adicional para a CONTRATANTE e entregues num prazo máximo de 30 (trinta) dia corridos contados da data de conclusão do projeto.

Os custos de instalação, manutenção e assistência técnica dos novos equipamentos que vierem a integrar a Infraestrutura de TIC serão de responsabilidade da CONTRATANTE.

1.2.10. Requerimentos para prestação de serviços

Para o caso de gerenciamento de serviços contínuos de tecnologia da informação e comunicação da FAPEMIG serão consideradas as melhores práticas da ITIL (*Information Technology Infrastructure Library*) e da ISO 20.000.

A contratada também deverá atender aos seguintes requisitos mínimos:

- Não haverá qualquer forma de subordinação dos prestadores de serviços alocados para as atividades com a CONTRATANTE;
- No prazo máximo de 30 (trinta) dias corridos após o início da vigência do contrato, a CONTRATADA deverá apresentar relação de profissionais com os quais possua vínculo profissional, para atendimento do contrato, devidamente habilitados, no mínimo, nas seguintes quantidades e com as certificações constantes no item 1.2.11.1.
- A comprovação do vínculo profissional se fará por meio da apresentação de cópia da Carteira Profissional (CTPS) em que conste a CONTRATADA como contratante, ou do contrato social da CONTRATADA em que conste o profissional como sócio, ou, ainda, do contrato de prestação de serviços com a CONTRATADA nos termos da legislação vigente;
- A CONTRATADA deverá enviar semestralmente ao Gestor do Contrato, juntamente com os relatórios gerenciais, listagem atualizada dos profissionais certificados, descriminando suas respectivas certificações;
- Quando solicitado pela CONTRATANTE, a CONTRATADA deverá fornecer todas as informações a respeito dos profissionais que irão prestar os serviços e de sua qualificação técnica, bem como deverá fornecer quaisquer outras informações que a CONTRATANTE solicite para comprovação de vínculo profissional dos prestadores de serviço;
- Caso a CONTRATADA precise substituir um profissional alocado para atendimento ao contrato, deverá informar à CONTRATANTE, com antecedência mínima de 5 (cinco) dias úteis, para que o novo profissional possa se inteirar dos procedimentos técnicos e administrativos para a boa execução dos serviços contratados, assegurando, em todos os casos, o atendimento ao previsto no item 1.2.6.2 deste Anexo, quanto ao perfil profissional e aos requisitos técnico profissionais para o profissional substituído;
- A CONTRATANTE poderá solicitar a substituição de prestador de serviço alocado para atendimento ao contrato, devendo o pedido ser formalizado até

5 (cinco) dias úteis, antes da substituição, que far-se-á obrigatoriamente, sob pena de incorrer a CONTRATADA em falta contratual;

- Todos os equipamentos e softwares fornecidos deverão contemplar a instalação, a configuração, os testes de desempenho, o suporte e a assistência técnica durante a vigência do contrato;
- Toda a infraestrutura de rede de dados, a saber: Switches Core, de Distribuição e de Acesso deverão ser do mesmo fabricante;
- Toda a infraestrutura de rede de dados, a saber: controladora wireless e Access Points deverão ser do mesmo fabricante;
- Todos os elementos ativos que vierem a ser ofertados ao longo do Contrato deverão ser compatíveis com os elementos ativos de rede em uso, deverão ser novos, sem uso anterior, sem previsão de encerramento de fabricação na data de entrega da proposta, não sendo aceita solução em *roadmap*;
- Todos os equipamentos e softwares fornecidos como resultado da prestação de serviços pela CONTRATADA serão de propriedade da CONTRATANTE e incorporados ao patrimônio da CONTRATANTE;
- Todos os produtos e artefatos gerados como resultado da prestação de serviços pela CONTRATADA serão de propriedade da CONTRATANTE, sendo vedada qualquer divulgação ou comercialização por parte da CONTRATADA, sem sua prévia autorização;
- Os produtos e artefatos gerados como resultado da prestação de serviços pela CONTRATADA deverão ser disponibilizados para a CONTRATANTE sempre que solicitado, no prazo máximo de 05 (cinco) dias úteis após a solicitação;
- Caso os equipamentos fornecidos pela CONTRATADA não se adequem aos racks disponíveis nas salas de telecomunicações, ela será responsável pelo fornecimento dos racks para toda a sua solução;
- A CONTRATADA deverá disponibilizar manual de instrução e operação de todos os equipamentos e softwares fornecidos;
- A CONTRATADA deverá documentar e disponibilizar todas as configurações realizadas nos equipamentos e sistemas que integram a Infraestrutura de TIC;
- Deverá ser fornecido documento declarando que, durante o período de garantia, a assistência técnica dos equipamentos e softwares será de inteira responsabilidade da CONTATADA, inclusive todos os seus custos, e que será prestada por empresa(s) autorizada(s) pelo fabricante;

- A CONTRATADA deverá ministrar treinamento oficial do fabricante, teórico e prático, para tornar os treinandos aptos a instalar, configurar e operar plenamente a solução fornecida e todas as funcionalidades especificadas neste Edital e em seus Anexos de acordo com as definições do projeto tecnológico. O treinamento deverá ser ministrado para, no mínimo, 2 (dois) técnicos da FAPEMIG e poderá ocorrer concomitantemente ao processo de instalação e configuração, o qual será de responsabilidade da CONTRATADA. Os treinamentos deverão ser realizados na cidade de Belo Horizonte - MG em local a ser disponibilizado pela CONTRATADA, que também será responsável pelos recursos necessários (instrutor, espaço físico, laboratório, equipamentos, material didático etc.);
- A CONTRATADA deverá fornecer documentação digital, em idioma português ou inglês, contendo orientações para configuração e operação de todos os equipamentos que venha a instalar durante a vigência do contrato.

1.2.11. Centro de Operações de Rede e Segurança

A contratada deverá possuir estrutura própria para a prestação dos serviços necessários ao gerenciamento centralizado da solução de rede de dados, disponível em qualquer ponto de presença no Brasil, com profissionais certificados, próprios ou de terceiros.

Deverá ser considerada uma estrutura mínima na região metropolitana de Belo Horizonte para intervenções e reparos, manutenções corretivas, diagnósticos, customizações, alterações físicas e funcionais e chamados nos equipamentos da rede local da FAPEMIG.

Para o Centro de Gerência Remoto, a conexão à rede da CONTRATADA deverá ser feita através de link dedicado, sob responsabilidade da CONTRATADA. Opcionalmente, a CONTRATADA poderá utilizar conexão VPN Internet, Frame Relay, PPP, HDLC ou MPLS. O acesso à Internet deverá ser controlado por meio de Proxy Server e permitido conforme os diferentes perfis dos operadores.

1.2.11.1. Equipe de operações

A contratada deverá possuir, pelo menos:

- dois (02) colaboradores com a certificação *Foundation Certificate in IT Service Management* (ITIL), ou similar, admitindo-se a comprovação de pelo menos

2.000h (duas mil horas) de experiência na função por meio de atestados de capacidade técnica emitidos por terceiro;

- um (01) colaborador para a solução de rede de dados e um (01) para segurança de rede, com a certificação do(s) fabricante(s) dos equipamentos fornecidos para a solução que ateste a capacitação dos colaboradores na instalação, configuração e operação dos serviços;
- um (01) colaborador com a certificação *Project Management Professional* (PMI), ou similar, admitindo-se a comprovação de pelo menos 2.000h (duas mil horas) de experiência na função por meio de atestados de capacidade técnica emitidos por terceiro.

1.2.11.2. Atividades da Equipe de Operação

A operação da rede de dados da CONTRATANTE exige a realização de diversas atividades de gestão, planejamento e manutenção que devem ser realizadas de forma coordenada entre a CONTRATADA e a CONTRATANTE, bem como entre os demais fornecedores de serviço da CONTRATANTE. As atividades apresentadas abaixo estão incluídas dentro do escopo de serviços a serem executados pela CONTRATADA:

- Gestão, monitoramento, manutenção e operação de toda a Infraestrutura de Rede de dados da CONTRATANTE;
- Gestão de mudanças na manutenção e nas manobras no cabeamento estruturado dos racks das Salas de Telecom e Data Center, incluindo o fornecimento de *patch cords* para espelhamento;
- Manutenção preventiva e corretiva em todo o ambiente operacional. A manutenção preventiva é feita com visitas periódicas a todas as Salas de Telecom e Data Center com o intuito de verificar suas condições operacionais, tais como limpeza, refrigeração e estado geral dos equipamentos e racks;
- Atendimento a chamados abertos pelos usuários da FAPEMIG. Os chamados chegam pela interface do software disponibilizado pela CONTRATANTE e devem ser tratados dentro do SLA de acordo com o item 1.2.6.2;
- Acompanhamento de intervenções na infraestrutura de comunicação de dados, elétrica, combate a incêndio, vigilância, *colocation* e de refrigeração das Salas de Telecom e Data Center (Core, Distribuição e Acesso);
- Atualização de software em todos os equipamentos do ambiente de rede de dados e segurança da CONTRATANTE. A atualização deve ser realizada

conforme recomendação do fabricante dos equipamentos e após aprovação e autorização da CONTRATANTE;

- A CONTRATANTE terá direito às atualizações (upgrades e updates) de todo e qualquer software dos equipamentos objeto deste Termo de Referência, incluindo versões de drivers ou firmwares, assinaturas de IPS e patches e correções, necessárias para o perfeito funcionamento dos equipamentos, durante todo o período de vigência do contrato, sem nenhum ônus adicional. No caso de um software ser descontinuado, deverá ser fornecida uma solução (Hardware e Software) completa que ofereça um nível de funcionalidade no mínimo igual ao provido pelo software descontinuado, sem nenhum custo adicional para a CONTRATANTE, devendo ser considerado os itens 1.2.7.I e 1.2.7.I.a;
- Apoio à equipe da CONTRATANTE nas definições de novos serviços e/ou necessidades, incluindo novos cenários e estudo de viabilidade técnica para avaliação destes cenários;
- Gestão do ambiente integrado da rede de dados da CONTRATANTE, sendo responsável pela aplicação e manutenção das políticas de segurança estabelecidas pela CONTRATANTE;
- Apoio aos demais fornecedores de serviços da CONTRATANTE para instalação de novos serviços e equipamentos, além da resolução de problemas. Todas as intervenções ou manutenções que afetem direta ou indiretamente a estrutura de rede de dados da CONTRATANTE devem ser acompanhadas pela equipe de operação da Rede;
- Consultoria e assessoramento à equipe da CONTRATANTE em questões necessárias para melhorias técnicas;
- Disponibilização de espaço e infraestrutura dentro dos racks localizados na FAPEMIG. Os racks que não contêm equipamentos de responsabilidade da CONTRATADA devem ser monitorados pela equipe de operação da Rede com o intuito de não ocorrerem desvios nos padrões de segurança e conectividade estabelecidos pela CONTRATANTE;
- Acompanhamento da ativação e desativação dos pontos de cabeamento horizontal pela equipe da CONTRATANTE. As atividades são realizadas nos racks presentes nas diversas Salas de Telecom e no Data Center da CONTRATANTE;
- Manutenção, manobras e organização dos racks localizados nas Salas de Telecom e Data Center da CONTRATANTE;

- Gestão do ambiente para paradas programadas e emergenciais, interagindo com os diversos fornecedores de serviços da CONTRATANTE no sentido de programar, documentar e minimizar os impactos provenientes destas paradas;
- Apoio aos diversos fornecedores de serviços da CONTRATANTE quando da necessidade de utilização da estrutura de rede, incluindo cabeamento horizontal e vertical, para outros serviços. Dentre eles:
    - CFTV;
    - Controle de Acesso de Pessoas e Automóveis;
    - Sonorização;
    - Relógios de ponto;
    - Automação predial;
    - Elevadores;
    - Sistema de iluminação;
    - Ar-condicionado;
    - Terminais de autoatendimento.
- Semestralmente, ou quando houver mudanças no ambiente, ou quando solicitado pela CONTRATANTE, a CONTRATADA deverá entregar caderno de testes, contendo o planejamento e a execução dos testes de funcionamento, performance, e redundância de todos os equipamentos que compõe a rede da FAPEMIG, com vistas a garantir e comprovar a alta disponibilidade.

1.2.11.3. Descrição do escopo

Toda a infraestrutura e operação da rede corporativa de dados da FAPEMIG deverão ser monitoradas e geridas constantemente através de um Centro de Operação composto de um COR (Centro de Operações de Rede) e um COS (Centro de Operações de Segurança), funcionalmente coordenados e integrados, garantindo a disponibilidade, qualidade, confiabilidade e segurança das informações e dispositivos suportados na rede.

O gerenciamento dos serviços prestados pelo Centro de Operações de Rede e de Segurança deverá obedecer às melhores práticas de gerenciamento de serviços seguindo o padrão ITIL (*Information Technology Infrastructure Library*).

O COR/COS será o responsável por implementar as diretrizes de segurança da informação definidas para todo o ambiente da rede corporativa da FAPEMIG.

O COR/COS deverá ter controle do inventário e fazer a gestão dos ativos de rede, permitindo à equipe de TI conhecer o perfil de atividades da rede, bem como controlar a sua utilização e promover alterações de forma proativa visando a melhoria contínua dos serviços prestados.

Esta unidade de controle poderá ser remota, mas deverá garantir a presença de técnicos na região metropolitana de Belo Horizonte de forma a garantir alta disponibilidade e rapidez na resolução de incidentes e na manutenção de:

- Equipamentos e demais ativos de rede;
- Sistemas e softwares fornecidos juntamente com a solução;
- Cabeamento lógico estruturado das Salas de Telecom e Data Center, contemplando as fibras ópticas, cabeamento UTP CAT 6 e patch cords.

O gerenciamento deve incluir ferramentas com acesso completo a partir das estações de trabalho da CONTRATANTE (até 03 acessos simultâneos) que possibilitem a gestão de alarmes, falhas, configuração, inventário e performance. O gerenciamento deverá ser centralizado e todos os eventos devem ser correlacionados, possibilitando uma visão completa de todos os elementos envolvidos nos eventos e daqueles identificados como causa raiz dos eventuais problemas de disponibilidade ou desempenho. Deverá permitir que todos estes eventos possam ser tratados pelos mesmos processos. O gerenciamento deverá ainda realizar análise de impacto, correlação de eventos e emissão de relatórios.

1.2.11.4. Requerimentos de operação

Para o gerenciamento da solução deverão ser obrigatoriamente implementados dois Centros de Gerência, sendo um remoto e um local (região metropolitana de Belo Horizonte).

Caberá à CONTRATADA o inteiro gerenciamento e dimensionamento da equipe responsável pela execução dos serviços, bem como a logística necessária, levando em conta os quantitativos contratados e os níveis de serviço exigidos.

Para o Centro de Gerência Local, deverá ser considerada uma estrutura mínima de técnicos na região metropolitana de Belo Horizonte para intervenções e reparos emergenciais, manutenções corretivas, diagnósticos, customizações, alterações físicas e funcionais e chamadas de criticidade elevada nos equipamentos da rede local. A equipe local deverá ser dimensionada de forma a garantir o pleno atendimento aos níveis de serviço definidos neste Termo de Referência e ser composta com no mínimo 02 (dois) profissionais.

Para o Centro de Gerência Remoto, a conexão à rede da licitante deverá ser feita através de link dedicado, sob a responsabilidade da CONTRATADA. Opcionalmente, a CONTRATADA poderá utilizar conexão VPN Internet, Frame Relay, PPP, HDLC ou MPLS. O acesso à Internet deverá ser controlado através de Proxy Server e permitido conforme os diferentes perfis dos operadores.

1.2.11.5. Centro de Operação da Rede (COR)

O Centro de Operações de Rede (COR) de Dados deverá ser composto por:

- Central de Monitoramento das Redes: Local onde ficarão os recursos humanos e os recursos de hardware/software responsáveis pelo monitoramento das redes;
- Plataforma de Monitoramento: composta de Sistemas Informatizados (hardware e software) a ser fornecido pela CONTRATADA;
- Plataforma de Gerenciamento da CONTRATADA: Recursos de hardware/software utilizados pela CONTRATADA para gerenciar os elementos de rede.

As responsabilidades do COR deverão ser as seguintes:

- Monitoramento e Coleta de Dados;
- Projeto de displays de status de rede;
- Detecção do problema (detecção do evento);
- Identificação do problema (detalhamento do problema);
- Diagnóstico do problema (análise de falha e plano de ações corretivas e preventivas);
- Resolução do problema;

- Testes sob produção;
- Roteamento dinâmico e alternativo em caso de falhas;
- "Network Recovery";
- Relatórios de Disponibilidade e Capacidade de todos ativos do ambiente;
- Interface com o Service Desk da CONTRATANTE;
- Avaliação das ferramentas no controle operacional da rede;
- Inventário dos equipamentos de rede.

A CONTRATADA deverá atender, no mínimo, às seguintes especificações relativas ao gerenciamento proativo dos serviços contratados:

- Possuir, em suas instalações, uma estrutura de operação e gerenciamento unificado da rede, até o último ponto. Isso significa que deverá ter total controle sobre todos os recursos que compõem a rede. Para tanto, deverá utilizar Software de Gerenciamento, que garanta, inclusive, a tomada de ações proativas.

1.2.11.6. Centro de Operações de Segurança (COS)

A CONTRATADA terá a responsabilidade de analisar os incidentes ou atividades e agir de forma proativa, garantindo a operação correta do sistema. Deverá monitorar os eventos de rede no ambiente da FAPEMIG e, caso algum incidente seja detectado, executar os procedimentos de resposta a incidentes e recuperação do ambiente.

A solução deverá cobrir quatro fases da monitoração dos processos:

- Detecção;
- Tratamento do incidente;
- Resposta ao incidente;
- Gerenciamento de infraestrutura.

O sistema utilizado pelo COS deverá ter as seguintes funcionalidades:

- Interface web;
- Integração com todos os sistemas de segurança utilizados na FAPEMIG, como antivírus, spam, IPS/IDS e firewall;
- Correlacionar as informações repassadas pelos dispositivos de segurança;

- Verificação de vulnerabilidades em sistemas Web.

1.2.12. Requerimento de planejamento e organização

A CONTRATADA deverá atender aos seguintes itens de planejamento e organização, de forma a garantir a efetividade da implantação e operação do objeto licitado.

1.2.12.1. Gerenciamento do Projeto

Para a transição da operação dos serviços, conforme descrito no item 1.2.4, a CONTRATADA, em conjunto com a CONTRATANTE, deverá nomear um Gerente de Projetos, capacitado para executar esta função, de acordo com o item 1.2.11.1, que será responsável por aplicar metodologia de gestão de projetos, coordenar as atividades de transição da operação contratada, garantir o cumprimento de todo o escopo e atividades previstas, estabelecer e executar o plano de comunicação com as áreas envolvidas, respondendo a CONTRATANTE sobre o progresso das atividades de transição, e implementar eventuais correções ao projeto. Este gerente, em conjunto com sua equipe, deverá planejar, executar e documentar as etapas previstas na transição da operação dos serviços, coordenar e priorizar as demandas e recursos, gerir conflitos, conduzir análise de risco e demais atividades necessárias à garantia do escopo e dos prazos de início de operação estabelecidos no cronograma apresentado no Termo de Referência.

Para atendimento a necessidade de transição dos serviços, a CONTRATADA deverá entregar um Plano de Gerenciamento de Projeto completo, em meio digital, no prazo máximo de 30 (trinta) dias após assinatura do contrato. Este plano de gerenciamento de projeto deverá conter no mínimo os seguintes itens:

- Planejamento do Escopo;
- Planejamento de Prazos;
- Planejamento de Recursos;
- Planejamento de Qualidade;
- Planejamento de Riscos;
- Planejamento de Comunicação;
- Planejamento de Aquisições;
- Planejamento de Integração.

1.2.12.2. Gerenciamento da Disponibilidade

O Gerenciamento da Disponibilidade tem por objetivo otimizar a capacidade da infraestrutura e ajudar a organização a entregar um nível sustentado de disponibilidade a um custo aceitável, que permita satisfazer os objetivos de negócio. O planejamento da manutenção de hardware é um aspecto importante do Gerenciamento da Disponibilidade e deve considerar os aspectos relativos a orçamentos, cronogramas de negócios e garantias.

As atividades assinaladas abaixo são de responsabilidade da CONTRATADA, devendo ser executadas integralmente em conjunto com todas aquelas atividades a elas relacionadas:

- Determinar um plano de manutenção abrangente e efetivo baseado nos requerimentos de nível de serviço (Parada Programada);
- Definir programação de manutenção;
- Coordenar as atividades de manutenção de equipamentos e sistemas do escopo deste edital;
- Resolver e/ou coordenar a resolução de problemas relacionados ao hardware localmente através do processo de mudança;
- Identificar a causa das indisponibilidades ocorridas e reportar mensalmente em relatórios gerenciais;
- Fazer a interface com os provedores de hardware para planejamento e resolução de problemas;
- Elaborar e manter um Plano de Gerenciamento de Disponibilidade apropriado e atualizado, que reflita as necessidades atuais e futuras do negócio;
- Prover informações sobre a disponibilidade de forma a garantir que se mensure e monitore de maneira contínua os níveis de serviços acordados de disponibilidade, confiabilidade, sustentabilidade e funcionalidade;
- Reduzir a frequência e a duração dos incidentes que incidam sobre a disponibilidade em um período determinado;
- Otimizar a disponibilidade da infraestrutura a fim de proporcionar melhoras de eficiência e aumento dos benefícios para o negócio e para a satisfação dos usuários;

O Plano de Gerenciamento de Disponibilidade deve ser entregue no prazo de 30 (trinta) dias corridos após o início da vigência do contrato.

A cada 180 (cento e oitenta) dias corridos após o início da vigência do contrato, o Plano de Gerenciamento de Disponibilidade deverá ser revisto e atualizado em comum acordo entre a CONTRATADA e a CONTRATANTE.

1.2.12.3. Gerenciamento da Capacidade

O objetivo do processo de Gerenciamento da Capacidade é compreender as necessidades futuras do negócio (a entrega de serviços necessária), a operação da organização (a entrega de serviços atual), a Infraestrutura de TIC (os recursos para a entrega de TIC) e garantir que todos os aspectos de capacidade e de desempenho, relacionados às necessidades do negócio atuais e futuras, sejam fornecidos com efetividade de custo.

O processo de Gerenciamento da Capacidade envolve três funções: o monitoramento, a modelagem e o planejamento, que visam garantir que os recursos tecnológicos estejam disponibilizados – na quantidade e qualidade necessárias – de forma a atender à carga de trabalho demandada pelo negócio, tais como facilidades de infraestrutura, processadores, armazenamento, meios de comunicação, entre outros. As atividades assinaladas abaixo são de responsabilidade da CONTRATADA, devendo ser executadas integralmente, em conjunto com todas aquelas atividades a elas relacionadas:

- Dar suporte no diagnóstico e na resolução de incidentes e problemas relacionados à questão de desempenho e capacidade;
- Garantir que o desempenho do serviço seja alcançado ou exceda todas as metas de níveis de serviços acordadas por meio do gerenciamento da capacidade dos serviços e dos recursos envolvidos;
- Monitorar a utilização da rede e de sua capacidade;
- Produzir relatórios sobre tendências de utilização de recursos para serem apresentados e terem seus resultados discutidos em reuniões mensais com a CONTRATANTE;
- Realizar análise de tendências com base nos relatórios de capacidade e desempenho;
- Prever necessidade de recursos com base em requerimentos de negócio;
- Avaliar configurações alternativas e recomendar soluções;
- Executar as atividades necessárias para monitorar a capacidade e o desempenho dos ambientes;

- Capturar e consolidar estatísticas sobre o desempenho do serviço e sobre a utilização dos recursos;
- Criar relatórios de desempenho;
- Isolar problemas de desempenho;
- Registrar mudanças feitas com propósito de ajustes (*tuning*);
- Monitorar mudanças feitas depois dos ajustes (*tuning*);
- Elaborar e monitorar o plano de capacidade apropriado e atualizado, refletindo as necessidades atuais e futuras de negócios;
- Avaliar o impacto de todas as mudanças no plano de capacidade e o desempenho e capacidade de todos os serviços e recursos;
- Garantir que medidas proativas sejam implantadas para melhoria dos serviços.

O Plano de Gerenciamento da Capacidade deve ser entregue no prazo de 30 (trinta) dias corridos após o início da vigência do contrato.

A cada 180 (cento e oitenta) dias corridos após o início da vigência do contrato, o Plano de Gerenciamento da Capacidade deverá ser revisto e atualizado em comum acordo entre a CONTRATADA e a CONTRATANTE.

1.2.12.4. Gerenciamento de Problemas

O processo de Gerenciamento de Problemas tem por objetivo minimizar o impacto adverso de Incidentes e Problemas no negócio, causados por erros na infraestrutura e evitar, de forma proativa, a ocorrência de incidentes, problemas e erros.

O Gerenciamento de Problemas envolve a análise de causa-raiz de um dado incidente e a identificação e aplicação de uma solução de contorno para este incidente ou, sempre que possível e, preferencialmente, de uma solução definitiva.

As atividades assinaladas abaixo são de responsabilidade da CONTRATADA, devendo ser executadas integralmente, em conjunto com todas aquelas atividades a elas relacionadas:

- Prover serviço de gerenciamento de problemas, incluindo registro, resolução e relatórios de acompanhamento para a Infraestrutura de TIC;

- Monitorar, resolver e produzir relatórios sobre os problemas no ambiente produtivo;
- Identificar e resolver problemas de acordo com procedimento formal estabelecido e coordenar os grupos de suporte até a resolução do problema.
- Identificar tendências de problemas e produzir relatórios de exceção;
- Conduzir análise de causa-raiz e fazer revisão dos problemas de alto impacto.
- Documentar a resolução de problemas;
- Identificar medidas preventivas e avaliar risco;
- Prover relatórios padronizados que devem incluir estatísticas sobre os problemas, os problemas significativos e o status dos problemas, de acordo com o processo definido.

O Plano de Gerenciamento de Problemas deve ser entregue no prazo de 30 (trinta) dias corridos após o início da vigência do contrato.

A cada 180 (cento e oitenta) dias corridos após o início da vigência do contrato, o Plano de Gerenciamento de Problemas deverá ser revisto e atualizado em comum acordo entre a CONTRATADA e a CONTRATANTE.

1.2.12.5. Gerenciamento de Configuração

O Gerenciamento de Configuração tem por objetivo fornecer um modelo lógico da Infraestrutura de TIC através da identificação, controle, manutenção e verificação das versões de todos os Itens de Configuração existentes. O relatório do Gerenciamento de Configuração deverá ser entregue mensalmente e/ou quando solicitado.

O Gerenciamento de Configuração efetivo mantém informações atualizadas sobre a Infraestrutura de TIC (hardware, software, licenças e documentação) e sobre os serviços vinculados a ela. Essas informações, contidas em um Banco de Dados de Gerenciamento da Configuração – BDGC (ou CMDB – *Configuration Management Database*), suporta os outros processos de Gerenciamento de Serviços de TIC em suas atividades do dia a dia. A fim de manter um BDGC exato e atualizado, é importante que, ao serem feitas mudanças na infraestrutura, os itens de configuração (ICs) associados também sejam registrados/atualizados no BDGC. Isso permite à organização ter melhor controle sobre a Infraestrutura de TIC, incluindo a monitoração e controle de licenças de software.

As atividades assinaladas abaixo são de responsabilidade da CONTRATADA, devendo ser executadas integralmente, em conjunto com todas aquelas atividades a elas relacionadas:

- Identificar e documentar os itens de configuração monitorados através da sua ferramenta de monitoramento;
- Cadastrar e manter registro e documentação atualizada dos IC's no BDGC.
- Fornecer informações necessárias à identificação dos IC's;
- Monitorar todos ativos, bem como seus atributos controláveis (Licenças, Tempo de Vida e atualizações).

A CONTRATADA deverá fornecer uma solução de CMDB para a CONTRATANTE e cadastrar nela todos os itens da infraestrutura de rede atual, relacionados nos itens 1.2.2.2 e 1.2.2.3, até 30 (trinta) dias corridos após o início da vigência do contrato. Os itens que virão a compor a solução que substituirá a infraestrutura atual, deverão ser cadastrados no CMDB no mínimo 5 (cinco) dias antes de substituírem os equipamentos da infraestrutura da FAPEMIG e se tornarem ativos no CMDB, salvo substituições emergenciais de equipamentos para restaurar a disponibilidade da rede.

1.2.12.6. Gerenciamento do Nível de Serviços

A CONTRATADA, em conjunto com a CONTRATANTE, deverá realizar o gerenciamento do nível de serviço, tendo como objetivos:

- Negociar e acordar os requisitos de nível dos serviços atuais e futuros alinhando as necessidades dos negócios;
- Desenvolver e gerenciar Acordo de Nível de Serviços (ANS);
- Prevenir proativamente falhas nos serviços;
- Reportar e gerenciar serviços para limitar brechas nos ANS;
- Elaborar o Plano de Melhoria de Serviços para gerenciar, planejar e implantar melhorias nos serviços e processos;
- Os acordos de nível de serviços devem conter no mínimo os seguintes conteúdos:
    - Descrição do serviço prestado;
    - Período de análise;

- Descrição breve das comunicações, incluindo relatórios;
- Detalhes de contato das pessoas autorizadas a agirem em emergências, participando na correção, recuperação ou solução temporária de incidentes e correções de problemas;
- Interrupções programadas e acordadas;
- Processo de notificação e escalada;
- Procedimento de reclamações;
- Metas do serviço;
- Limites de carga de trabalho;
- Ações a serem tomadas em caso de interrupção do serviço (contingência).

A qualquer momento, durante a execução do contrato, as metas (ANS), indicadores, produtos e demais elementos que impactam na forma de pagamento poderão ser revistos e ajustados pelas partes.

1.2.12.7. Gerenciamento de Incidentes

O objetivo do processo de Gerenciamento de Incidentes é restabelecer a operação normal do serviço o mais rapidamente possível, com o mínimo de interrupção do negócio, assegurando assim que os melhores níveis de disponibilidade sejam mantidos.

A CONTRATADA, em conjunto com a CONTRATANTE, e com os outros fornecedores de serviços de TIC na FAPEMIG serão parte de um processo macro de incidentes a ser definido pela CONTRANTE. A CONTRATADA será a responsável pelo processo de gerenciamento de incidentes do escopo contratado. As atividades assinaladas abaixo são de responsabilidade da CONTRATADA, devendo ser executadas integralmente, em conjunto com todas aquelas atividades a elas relacionadas:

- Detectar incidente por meio da gestão de eventos praticadas pelo Centro de Operações de Rede e Segurança, registrá-los (cadastrá-los) na ferramenta oficial da CONTRATANTE e tratá-lo de acordo com os acionamentos necessários;
- Prover serviço de gerenciamento de incidentes do escopo contratado, incluindo tratativa de incidentes, escalação, resolução e relatórios de

acompanhamento para a Infraestrutura de TIC, de acordo com o processo estabelecido;

- Monitorar, resolver e produzir relatórios sobre os incidentes no ambiente;
- Escalar incidente de acordo com procedimento formal estabelecido e coordenar os grupos de suporte e provedores até a resolução do incidente;
- Identificar tendências de incidentes e produzir relatórios de exceção;
- Documentar a resolução dos incidentes;
- Prover relatórios padronizados mensalmente e/ou quando solicitado sobre os incidentes, apresentando estatísticas sobre o total de incidentes, os incidentes significativos e o status dos incidentes, de acordo com o processo definido;
- Acionar fornecedores de equipamentos e tratar fim-a-fim os incidentes relativos ao hardware dos equipamentos relacionados ao contrato reportando à CONTRATANTE o andamento da solicitação aberta com os fornecedores;
- Acionar fornecedores de infraestrutura de dados e tratar fim-a-fim os incidentes relativos aos links de dados reportando à CONTRATANTE o andamento da solicitação aberta com os fornecedores;
- Acionar fornecedores de infraestrutura elétrica e registrar acionamento na ferramenta da CONTRATANTE de gestão de chamados;
- Acompanhar o tratamento de incidentes na infraestrutura elétrica junto aos fornecedores responsáveis por ela;
- Registrar incidentes na infraestrutura de refrigeração na ferramenta da CONTRATANTE de registro de chamados;
- Acompanhar o tratamento de incidentes na infraestrutura de refrigeração junto aos fornecedores responsáveis por ela.

1.2.12.8. Gerenciamento de Eventos

A CONTRATADA será responsável pela gestão de eventos, provindas do COR (Centro de Operações de Rede) e COS (Centro de Operações de Segurança), durante todo o período de vigência do contrato. O objetivo é detectar todas as mudanças de estado dos Itens de Configuração (IC) monitorados, determinar as ações de controle adequadas e garantir que estas são comunicadas às funções apropriadas, fornecendo meios para comparar o desempenho operacional real e comportamento previsto.

As atividades assinaladas abaixo são de responsabilidade da CONTRATADA, devendo ser executadas integralmente, em conjunto com todas aquelas atividades a elas relacionadas:

- Monitorar toda rede da CONTRATANTE dentro do escopo contratado, e entregar mensalmente e/ou quando solicitado, relatório com informações sobre os ativos de rede (utilização de processamento, memória, consumo de rede, prospecção de utilização etc.);
- Registrar incidentes relacionados à rede da CONTRATANTE de acordo com o processo de incidentes de monitoramento que será definido pela CONTRATADA e submetido à aprovação da CONTRANTE;
- Detectar, filtrar, registrar, classificar e analisar mensagens baseados em filtros e limites de operação pré-estabelecidos;
- Gerenciar consoles de sistema, incluindo, mas não se limitando a monitoração, intervenção mediante mensagens, inicialização e shutdown etc.
- Interpretar e atuar perante mensagens de erro conforme requerido;
- Prover prontamente notificação sobre interrupções da rede conforme procedimento, que será definido pela CONTRATADA e submetido à aprovação da CONTRATANTE.

1.2.12.9. Gerenciamento de Mudanças

O processo de Gerenciamento de Mudanças tem por objetivo assegurar que métodos e procedimentos padronizados sejam utilizados para um tratamento eficiente e rápido de todas as mudanças, de forma a eliminar o impacto de eventuais incidentes sobre os serviços;

Para operação dos serviços, a CONTRATADA deverá realizar o gerenciamento de mudanças tendo como objetivo assegurar que as mudanças sejam feitas de forma controlada, avaliadas, priorizadas, planejadas, testadas, implantadas e documentadas;

As atividades assinaladas abaixo são de responsabilidade da CONTRATADA, devendo ser executadas integralmente, em conjunto com todas aquelas atividades a elas relacionadas:

- Controlar mudanças e atividades necessárias para implantar, configurar, mover, atualizar, repor e migrar itens de configuração;

- Criar, manter, documentar e distribuir uma programação futura de mudanças;
- Manter procedimentos e métodos padronizados para mudança;
- Especificar, documentar e manter o processo de mudanças;
- Produzir relatórios de status das mudanças programadas;
- Implementar mudanças de uma maneira organizada e consistente, seguindo os procedimentos do processo definido;
- Minimizar qualquer interrupção de serviço causada por mudanças, desde que tenha sido devidamente submetida ao processo de gerenciamento de mudanças;
- Medir e produzir relatórios sobre a atividade de mudanças e correlacionar com o processo de gerenciamento de problemas;
- Melhorar continuamente a efetividade do processo, fazendo com que mudanças bem-sucedidas sejam uma característica confiável e repetitiva do ambiente;
- Assegurar que existam planos de remediação caso as mudanças falhem.

1.2.12.10. Gerenciamento de Segurança

O Gerenciamento da Segurança da Informação envolve as atividades de planejamento, determinação de requerimentos, implementação, administração e revisão dos controles de segurança de forma a responder a eventos de segurança. O relatório do Gerenciamento de Segurança deverá ser entregue mensalmente e/ou quando solicitado.

As atividades assinaladas abaixo são de responsabilidade da CONTRATADA, devendo ser executadas integralmente, em conjunto com todas aquelas atividades a elas relacionadas:

- Prover acesso para sistemas, redes e aplicativos do escopo contratado;
- Seguir padrões de segurança da informação, diretrizes e procedimentos de aprovação de ID;
- Criar e apagar contas/perfil de usuários dentro do escopo de serviços contratados;
- Seguir as políticas e procedimentos de segurança da CONTRATANTE durante o acesso aos ambientes;

- Manter software de segurança;
- Reinicializar senhas de acordo com procedimentos aprovados;
- Entrar em contato com usuários para esclarecer requisições de administração de IDs;
- Identificar vulnerabilidades de segurança.

1.2.12.11. Monitoramento e Análise dos Serviços

Para a operação dos serviços, a CONTRATADA, em conjunto com a CONTRATANTE, deverá elaborar mensalmente relatório de monitoramento, mensuração, análise e revisão dos serviços incluindo no mínimo os seguintes itens:

- Desempenho comparado com as metas de nível de serviço;
- Não conformidades em relação aos padrões:
    - Quantidade de incidentes;
    - Incidentes dentro e fora do prazo;
    - Indicador por tipo de incidente;
    - Taxa de solução remota x campo;
    - Disponibilidade dos equipamentos no período.
- Desempenho após implementação de mudanças nos serviços;
- Informações sobre características e volume da carga de trabalho atual;
- Informação sobre tendências de consumo por período;
- Relatórios que apontem cargas de trabalho futuras e programadas:
- Ações corretivas;
- Ações preventivas;
- Ações de melhorias (SIP – Service Improvement Program);
- Atividades em andamento (status do plano de ação, se houver).
- Relatórios sobre vulnerabilidades de segurança;
- Atividades concluídas.

2. Dos lotes

2.1. Do agrupamento dos itens em lote

A composição do lote do objeto e seus quantitativos estimados estão especificados na tabela apresentada no item 1.

Justifica-se a necessidade de lote único, pois a existência de empresas distintas na execução do contrato pode colocar em risco a operação e dificultar a medição dos serviços. Para que não haja prejuízo para os fornecedores, o objeto foi definido de forma a manter a competitividade, o qual, não restringe qualquer participante, pois a seleção da proposta mais vantajosa à administração pública irá ocorrer naturalmente, mantendo-se os requisitos mínimos para garantir a execução do contrato, a segurança e a perfeição no cumprimento do objeto.

2.2. Lotes exclusivos para microempresas e empresas de pequeno porte

A participação na presente licitação é aberta a todos licitantes - **Licitação com participação ampla**, uma vez que o valor orçado pela Administração excede o limite que garante exclusividade às licitantes enquadradas como ME e EPP, exposto no Art. 48, inciso I, da LC 123/2006 c/c art. 8º do Decreto Estadual nº 47.437/2018.

3. Justificativa da contratação

Trata-se de licitação para a contratação dos serviços de infraestrutura de rede de dados, segurança, controle de acesso, nobreaks e gerador, incluindo o fornecimento de todos os equipamentos, softwares, licenças e demais insumos necessários à operação dos serviços na FAPEMIG, conforme especificações técnicas e condições comerciais previstas neste Edital e em seus Anexos.

Tendo em vista a necessidade de continuidade dos serviços ora existentes, o fato do prazo de garantia junto ao fornecedor dos equipamentos que compõe a infraestrutura de rede de dados atual da FAPEMIG ter se encerrado em 2017, e esta Fundação não possuir corpo técnico em quantidade nem expertise necessárias para esse tipo de suporte, nem ter condições de prever o tipo de problema ou demandas que podem ocorrer, justifica-se a necessidade de contratação de empresa que forneça o objeto proposto.

É importante destacar que todos estes equipamentos da rede atual da FAPEMIG já tiveram sua venda descontinuada pelo fabricante. Além disso, o ciclo de suporte ou ciclo de vida - indicativo de que o produto está no fim da sua vida útil ou que será descontinuado - desses equipamentos ou já se encerrou ou está próximo ao fim, justificando, portanto, a substituição dos equipamentos em detrimento à renovação/extensão de garantia junto ao fabricante nesta licitação.

4. Justificativa da modalidade

Os serviços a serem contratados nesta licitação enquadram-se no conceito de serviço comum, devido à natureza e complexidade de sua execução, e por serem descritos minuciosamente neste Termo de Referência, por meio de especificações usuais de mercado, evitando ainda propostas com grau de incerteza em relação ao objeto licitado.

Considerando as atividades desempenhadas pelos cerca de 250 (duzentos e cinquenta) colaboradores da FAPEMIG, cabe salientar que o serviço contratado é de natureza contínua, bem como de serviço auxiliar, imprescindível à Administração para o desempenho de suas atribuições, e, portanto, sua interrupção pode comprometer a continuidade das atividades da instituição. O serviço contratado realiza a segurança e permite o tráfego de dados para todos os colaboradores da FAPEMIG, sendo indispensável para seu acesso à internet, à rede corporativa, aos sistemas da FAPEMIG e do Estado, ao serviço de telefonia, dentre outros.

Nesse sentido, há necessidade da prestação do serviço descrito por mais de um exercício financeiro, com contratação prevista para a vigência de 36 (trinta e seis) meses. Este período de vigência foi escolhido por ser o mais vantajoso para a Administração, considerando que 12 (doze) ou 24 (vinte e quatro) meses seria um prazo curto para o investimento necessário da CONTRATADA para a operação. Considerando o modelo proposto, no qual os equipamentos instalados pela CONTRATADA serão novos e com ciclo de vida ativo junto ao fabricante, só teremos a substituição de equipamentos em casos de defeito, o que diminui o risco para a CONTRATADA no planejamento do investimento. Por outro lado, é importante ser destacada a obsolescência da tecnologia a ser implantada e os riscos em questões de segurança da informação (vulnerabilidade) que isso representa em se tratando de equipamentos de tecnologia da informação. Dessa forma, não é recomendável tecnicamente manter a solução funcionando durante um longo período.

Tendo em vista que a FAPEMIG busca que toda a infraestrutura de rede de dados (wired e wireless), segurança e controle de acesso funcione de forma totalmente integrada, faz-se necessária a contratação de uma única empresa para a prestação dos serviços previstos neste documento de forma a garantir o monitoramento e o gerenciamento adequados de todo o ambiente, sem prejuízo aos usuários. A contratação de mais de uma empresa poderia inviabilizar a operação, principalmente nos momentos em que seja necessária uma atuação contundente da CONTRATADA na busca da identificação e da solução de eventuais problemas.

Ao término do contrato e/ou quando solicitado pela CONTRATANTE, a CONTRATADA se obriga a entregar toda a documentação referente à operação e gerenciamento de todos os equipamentos que compõe a rede FAPEMIG, incluindo todas as configurações, alterações, senhas, regras, códigos-fonte, AS-BUILT, descrição completa de cada solução etc.

5. Participação de consórcios

Não será permitida a participação de empresas reunidas em consórcios, devido à baixa complexidade do objeto a ser adquirido, considerando que as empresas que atuam no mercado têm condições de fornecer os serviços de forma independente.

6. Qualificação técnica

I. A licitante deverá apresentar atestados de capacidade técnica emitidos por entidade pública ou privada, comprovando sua aptidão técnica para a realização dos serviços especificados. Deverão ser apresentados, no mínimo, os seguintes atestados de capacidade técnica:

   a. Pelo menos 01 (um) atestado de capacidade técnica, emitido por instituição pública(s) ou privada(s), comprovando a prestação de serviços de operação, manutenção preventiva, manutenção corretiva, gerenciamento e monitoramento de uma infraestrutura de rede de dados (wired e wireless) através de ativos de rede, com o objetivo de suportar, no mínimo, 432 (quatrocentos e trinta e dois) pontos de rede e, pelo menos, 75 (setenta e cinco) usuários.

      i. Deverá ser comprovado o quantitativo mínimo dos seguintes ativos de rede existentes na infraestrutura de rede: 1 (um)

Switch Core; 1 switch de Distribuição (*layer* 3) e; 10 (dez) switches de Acesso (*layer* 2).

b. Pelo menos 01 (um) atestado de capacidade técnica, emitido por instituição pública(s) ou privada(s), comprovando a prestação de serviços de operação, manutenção preventiva, manutenção corretiva, gerenciamento e monitoramento de infraestrutura de segurança composta por next generation firewall e NAC/ACS (Network Access Control/Access Control Server), para prover segurança de, no mínimo, 75 (setenta e cinco) usuários.

c. 01 (um) atestado de capacidade técnica, emitido por instituição pública(s) ou privada(s), comprovando a prestação de serviços de operação, manutenção preventiva, manutenção corretiva, gerenciamento e monitoramento de uma infraestrutura de rede sem fio indoor, com gerência e configuração centralizada. Deverá ser comprovado o quantitativo mínimo dos seguintes itens: 15 (quinze) Access Points, 1 (uma) Controller e Software de Gerência Wireless.

II. Os atestados de capacidade técnica deverão conter:

- Razão social e os dados de identificação da instituição emitente (CNPJ, endereço, telefone);
- Um breve resumo do escopo dos serviços realizados;
- Afirmação de que a licitante atendeu à solicitação do quantitativo e das condições de fornecimento e prestação do serviço de forma satisfatória;
- Local e data de emissão;
- Nome, cargo, telefone e a assinatura, com firma reconhecida, do responsável pelas informações.

7. Critérios de aceitabilidade da proposta

I. Será exigido o envio de Datasheet, em meio físico ou eletrônico, para fins de comparação entre a especificação descrita no Anexo III – Especificação dos ativos de rede, e o equipamento a ser disponibilizado pelo fornecedor.

8. Da execução do objeto

8.1. Prazo para a prestação dos serviços

I. A CONTRATADA deverá elaborar cronograma, a ser entregue em até 30 dias corridos após o início da vigência do contrato contendo detalhamento do serviço e produtos a serem utilizados, indicando os respectivos locais para a execução, observando:

   a. Início das atividades:

      i. 30 (trinta) dias corridos para a entrega dos Planos de Gerenciamento;

      ii. 60 (sessenta) dias corridos para o início da ativação da solução.

8.2. Do local para prestação dos serviços

I. Os serviços serão prestados no seguinte endereço: Avenida José Cândido da Silveira, 1500, bairro Horto, Belo Horizonte, Minas Gerais, CEP 31035-536;

II. O Centro de Operações e Segurança da Rede deve possuir ambiente remoto e local (Região Metropolitana de Belo Horizonte), em localidade decidida pela CONTRATADA;

III. Será disponibilizado um espaço máximo de 25 (vinte e cinco) m² na FAPEMIG, com suporte a aproximadamente 4 (quatro) pessoas, em caso de necessidade da CONTRATADA de estrutura local.

   a. O espaço será disponibilizado juntamente com pontos de rede local, pontos de energia elétrica e mobiliário (mesas e cadeiras). Quaisquer outros itens necessários ao funcionamento do ambiente e à execução das atividades serão de responsabilidade da CONTRATADA. Havendo a necessidade de alteração do espaço por parte da CONTRATADA, esta deverá solicitar formalmente à administração da FAPEMIG autorização para execução de qualquer intervenção ao espaço fornecido.

IV. O horário de funcionamento do Centro de Operações e Segurança da Rede e, consequentemente, o horário de prestação dos serviços, será de 07h00min (sete horas) às 19h00min (dezenove horas), de segunda a sexta-feira, em horário comercial, e de 19h01min (dezenove horas e um minuto) às 06h59min (seis horas e cinquenta e nove minutos) de segunda a sexta-feira e aos

sábados, domingos e feriados em horário integral, em horário de plantão. Ou seja, a operação será do tipo 24x7x365;

V. A disponibilidade da infraestrutura deverá seguir o regime de operação do tipo 24x7x365.

8.3. Condições de recebimento

I. O recebimento/aprovação dos serviços pela FAPEMIG não exclui a responsabilidade civil do fornecedor por vícios de quantidade ou qualidade dos serviços ou disparidades com as especificações estabelecidas, verificadas posteriormente, garantindo-se a Administração as faculdades previstas no art. 18 da Lei n° 8.078/90;

II. Todo o procedimento de fornecimento, instalação, configuração e operação na FAPEMIG será acompanhado e validado pelo Gestor do Contrato;

III. Todos os ativos fornecidos para a execução dos serviços contratados serão verificados quanto ao cumprimento das especificações e das funcionalidades requeridas no Anexo III – ESPECIFICAÇÕES DOS ATIVOS DE REDE à data de início de operação e durante todo o período de vigência do contrato;

IV. Os ativos serão recebidos:

   a. Provisoriamente, no ato da prestação

   b. Definitivamente, após a verificação da qualidade e quantidade da prestação e consequente aceitação, que deverá acontecer em até 10 dias úteis, contados a partir do recebimento provisório

V. Durante todo o período de vigência do contrato, o gestor poderá realizar auditorias para identificar eventuais divergências entre os serviços licitados e os empregados na operação.

8.3.1. Procedência e valor real dos ativos

Todos os ativos fornecidos para a composição da solução, durante a execução do contrato, deverão ser apresentados juntamente com o documento fiscal correspondente. Além disso, os produtos deverão vir acompanhados por documento emitido pelo fabricante indicando os produtos fornecidos e os seus respectivos números de série.

9. Do pagamento

9.1. Remuneração

I. O valor de remuneração mensal deverá ser calculado de acordo com a fórmula a seguir:

$$VRM = (QIC \times VU)1 + (QIC \times VU)2 + ... + (QIC \times VU)n$$

- Onde:
  - VRM = Valor Regular Mensal
  - QIC = Quantidade de Itens de Configuração cadastrados no CMDB
  - VU = Valor Unitário para cada item de Configuração

II. Para composição da fórmula, deverão ser considerados os diferentes itens de configuração e seus respectivos preços unitários. O termo (QIC x VU) será repetido tantas vezes quantas forem necessárias para referenciar todos os itens de configuração que sejam objeto do contrato;

III. A variável QIC (Quantidade de Itens de Configuração cadastradas no CMDB) refere-se aos itens de configuração que possuem o status ATIVO, onde:

a. ATIVO = item de configuração em uso;

b. INATIVO = item de configuração fora de operação.

IV. Os itens de configuração cadastrados no CMDB que não façam parte do objeto do contrato não serão considerados para apuração da variável QIC (Quantidade de Itens de Configuração cadastrados no CMDB).

9.2. Efetivação do pagamento

I. O pagamento será efetuado através do Sistema Integrado de Administração Financeira – SIAFI/MG, por meio de ordem bancária emitida por processamento eletrônico, a crédito do beneficiário em um dos campos que o fornecedor indicar, no prazo de até 30 (trinta) dias corridos, contados a partir da data final do período de adimplemento a que se referir, com base nos documentos discais devidamente conferidos e aprovados pela CONTRATANTE.

II. Na ocorrência de necessidade de providências complementares por parte da CONTRATADA, o decurso de prazo para pagamento será interrompido, reiniciando-se a contagem a partir da data em que estas forem cumpridas, caso em que não será devida atualização financeira.

III. O cálculo do valor devido por mês pela prestação do serviço corresponderá ao seguinte modelo de precificação:

a. O modelo de remuneração é o modelo que define o valor a ser recebido pela CONTRATADA, ao final de cada mês, referente aos serviços prestados. A remuneração é variável, de acordo com a quantidade de equipamentos cadastrados no Configuration Management Database (CMDB) e compatível com o serviço prestado e sua qualidade, sendo calculada por meio da seguinte fórmula (VPM):

i. O cálculo do valor de pagamento mensal (VPM):

$$VPM = VRM \times MFA$$

- Onde:
  - VPM = Valor de Pagamento Mensal
  - VRM = Valor Regular Mensal (valor definido no item 7.4)
  - MFA = Média das Faixas de Ajuste = (M1 + M2 + M3 + M4 + M5)/5
  - M1, M2, M3, M4 e M5 são as faixas de ajuste no pagamento, calculadas conforme o item 1.2.6.2

b. A CONTRATADA, no 3º (terceiro) dia útil de cada mês, enviará ao Gestor do Contrato, em meio eletrônico, os relatórios para controle dos níveis de serviço do mês anterior (item 1.2.6.2 observado o modelo de precificação previsto no item 9.2.II.a;

c. Os relatórios serão verificados pelo Gestor do Contrato no prazo de 05 (cinco) dias úteis e, estando em conformidade com o serviço efetivamente prestado e com os níveis de serviço estabelecidos, e não havendo qualquer outro impedimento, será autorizada, formalmente, a emissão da fatura e nota fiscal dos serviços prestados.

10. Do contrato

I. Encerrado o procedimento licitatório, o representante legal do licitante declarado vencedor será convocado para firmar o termo de contrato, aceitar ou retirar o instrumento equivalente, de acordo com os arts. 62, da Lei 8.666/93 e art. 4°, XXI, da Lei 10.520/2002.

II. O contrato a ser firmado entre as partes terá vigência de 36 (trinta e seis) meses, a partir da data de publicação de seu extrato no Diário Oficial do Estado de Minas Gerais, podendo ser prorrogado por idêntico período até o limite máximo de 60 (sessenta) meses, mediante celebração de termos aditivos, conforme dispõe o art. 57, II, da Lei n° 8.666/93.

    a. Poderá ser prorrogado , nos termos do item 10.II, apenas as parcelas do serviço caracterizadas como contínuas, discriminadas a seguir: Serviços de operação, atualização das soluções, gerenciamento, monitoramento, treinamento, suporte técnico, manutenção preventiva e manutenção corretiva de toda a infraestrutura de rede de dados (wired e wireless), segurança, controle de acesso, nobreaks e gerador.

III. Durante o prazo de vigência, os preços contratados poderão ser reajustados monetariamente com base no IPCA, observado o interregno mínimo de 12 (doze) meses, contados da apresentação da proposta, conforme disposto na Resolução Conjunta SEPLAG/SEF n°8.898/2013 e nos arts. 40, XI, e 55, III, da Lei n° 8.666/93, exclusivamente para obrigações iniciadas e concluídas após a ocorrência da anualidade.

    a. O direito a que se refere o item 10.III deverá ser efetivamente exercido mediante pedido formal da contratada até 180 (cento e oitenta) dias após o atingimento do lapso de 12 (doze) meses a que se refere o caput desta cláusula sob pena de preclusão do direito ao seu exercício;

    b. Os efeitos financeiros retroagem à data do pedido apresentado pela contratada;

    c. Nos reajustes subsequentes ao primeiro, manter-se-à o marco inicial descrito no item 10.III

    d. Desde que devidamente justificado e expressamente previsto no termo aditivo, o direito ao reajuste poderá ser exercido em momento posterior, até o encerramento do vínculo contratual.

IV. O prazo de vigência do contrato será de 36 (trinta e seis) meses, a partir da publicação do seu extrato na imprensa oficial. O período de execução do contrato dar-se-á concomitantemente ao de vigência.

V. Serão admitidas supressões ou adições contratuais até o limite de 25% do valor total do contrato, conforme art. 65, §1° da Lei 8.666/93

    a. A CONTRATADA deve estar atenta à possibilidade de adições contratuais de até 25% do valor total do contrato, no sentido de se

ampliar o escopo dos serviços fornecidos, em termos de infraestrutura fornecida, tanto em equipamentos, quanto em capacidade durante o prazo de vigência de contrato. Assim, a CONTRATADA deve optar por utilizar equipamentos com capacidade de expansão.

11. Procedimentos de fiscalização e gerenciamento da relação jurídica

I. Atendendo às exigências contidas no inciso III do art. 58 e §§ 1º e 2º, do artigo 67 da Lei nº. 8.666 de 1993, será designado pela autoridade competente, agente para acompanhar e fiscalizar o contrato, como representante da Administração.

   a. Será designado o servidor: Flávio Henrique Belo Rodrigues/MASP 753008-2

II. Em caso de eventual irregularidade, inexecução ou desconformidade na execução do contrato, o agente fiscalizador dará ciência à CONTRATADA, por escrito, para adoção das providências necessárias para sanar as falhas apontadas;

III. A fiscalização de que trata esta cláusula não exclui, nem reduz a responsabilidade da CONTRATADA por quaisquer irregularidades, inexecuções ou desconformidades havidas na execução do objeto, aí incluídas imperfeições de natureza técnica ou aquelas provenientes de vício redibitório, como tal definido pela lei civil;

IV. A CONTRATANTE reserva-se o direito de rejeitar, no todo ou em parte, o objeto da contratação, caso este se afaste das especificações do Edital, seus anexos e da proposta da CONTRATADA;

V. As decisões e providências que ultrapassarem a competência do Fiscal do Contrato serão encaminhadas à autoridade competente da CONTRATANTE para adoção das medidas convenientes, consoante disposto no § 2º do art. 67, da Lei nº. 8.666/93.

   a. Caberá ao gestor os controles administrativos/financeiros necessários ao pleno cumprimento do contrato.

12. Dotação orçamentária

A despesa decorrente desta licitação correrá por conta da dotação orçamentária do orçamento em vigor, aprovado pela Lei Orçamentária Anual, de 9 de janeiro de 2019:

<inserir dotação orçamentária>

13. Das garantias

13.1. Garantia de execução

I. Considerando a complexidade da contratação deverá ser prestada garantia contratual da licitante nos seguintes termos e condições:

a. Após a assinatura do contrato o licitante deverá apresentar, no prazo máximo de 10 (dez) dias corridos, contados da data da entrega da via do contrato assinada, comprovante de prestação de garantia correspondente a 5% sobre o valor global do contrato, e válida por todo seu período de vigência, em conformidade com o disposto no §2º do art. 56 da Lei Federal nº. 8.666/93;

b. A garantia prestada será liberada após o cumprimento integral de todas as obrigações contratuais, ficando a CONTRATANTE autorizada a executá-la para cobrir multas sancionatórias, indenização a terceiros ou pagamento de qualquer obrigação, inclusive em caso de rescisão, de responsabilidade da licitante vencedora;

c. A licitante vencedora se obriga a manter o valor da garantia em compatibilidade com o percentual estabelecido no subitem 13.1.I.a deste Termo de Referência, relativamente ao valor atualizado do contrato, devendo promover essa complementação de garantia e apresentar ao CONTRATANTE no prazo de até 10 (dez) dias, contados a partir da publicação do extrato do respectivo Termo Aditivo ou do registro do Termo de Apostila;

d. Havendo garantia, após a execução deste contrato, competirá à licitante vencedora formular à CONTRATANTE o pedido de liberação ou restituição;

e. O pedido de que trata este item será submetido a regular procedimento junto à CONTRATANTE, para fins da ordem de autorização;

f. Decorridos 5 (cinco) dias úteis da publicação da decisão favorável ficará franqueado à licitante proceder junto à unidade financeira do CONTRATANTE o levantamento da garantia;

g. A liberação ou restituição da garantia pelo CONTRATANTE, prestada em qualquer modalidade, somente se efetivará após sua deliberação favorável nos termos do artigo 56, § 4º da Lei nº 8.666, de 1993;

h. A CONTRATANTE, no decorrer da execução contratual, poderá autorizar a substituição da garantia inicialmente ofertada se, cumulativamente:

   i. A licitante comunicar ao CONTRATANTE prévia e justificadamente essa intenção;

   ii. O gestor do contrato por parte do CONTRATANTE declarar inexistir descumprimento de cláusula contratual de responsabilidade da CONTRATADA, bem como inexistir pendências relativas à execução do objeto e qualquer procedimento administrativo visando à apuração de responsabilidade da CONTRATANTE;

   iii. A substituição seja por modalidade estabelecida no §1º do art. 56 da Lei Federal nº 8.666, de 1993;

   iv. A nova garantia prestada preencher os requisitos do ato convocatório e deste Edital de licitação;

   v. No caso de Fiança e Seguro-Garantia exista expressamente prevista a cobertura de eventual inadimplência ocorrida na vigência da garantia substituída, ainda que o fato venha a ser apurado posteriormente ou, ainda, a garantia substituta tenha vigência igual à da substituída.

i. A não prestação de garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa.

13.2. Garantia do produto/serviço: fabricante, garantia legal ou garantia convencional

I. Todos os equipamentos e softwares da infraestrutura de rede de dados da FAPEMIG que compõem a rede atual, deverão possuir serviços de manutenção

durante toda a vigência do contrato, incluindo-se todos e quaisquer custos envolvidos na prestação deste serviço;

II. Todos os equipamentos e softwares da infraestrutura de rede de dados da FAPEMIG, que vierem a ser instalados ou substituídos deverão possuir garantia, assistência técnica e serviços de manutenção durante toda a vigência do contrato, incluindo-se todos e quaisquer custos envolvidos na prestação deste serviço.

14. Da vistoria técnica

I. Durante o período de elaboração das propostas, os licitantes poderão realizar vistoria técnica na área onde os serviços serão prestados, de forma a terem conhecimento da infraestrutura, dos tipos de serviços a serem prestados e das suas condições de execução;

II. A vistoria técnica será realizada nas seguintes condições:

a. Nos dias XX/XX/20XX às XX:XX, XX/XX/20XX às XX:XXh e XX/XX/20XX, às XX:XXh.

b. O fornecedor que desejar realizar visita técnica deverá agendar dia e horário específico, até 02 (dois) dias antes da sessão, sendo vedada a visita de mais de um fornecedor no mesmo momento;

c. Serão admitidos no máximo 2(dois) representantes por empresa licitante e não será permitido o registro de imagens durante a visita;

d. Para agendar visita à FAPEMIG, o licitante deverá entrar em contato com XXXXX no e-mail xxxxxx@fapemig.br ou pelo telefone (xx) 3280-2xxx, para indicação do(s) representante(s) da empresa que fará(ão) visita à FAPEMIG e escolha do dia da visita;

e. No dia agendado, o(s) representante(s) indicados deverá(ão) portar identificação original com foto e declaração autorizando-os (nome e RG) a realizar a visita técnica. Essa declaração deve ser assinada pelo representante legal da licitante, conter seu nome e RG e ser impressa em papel timbrado com o CNPJ da empresa;

f. Os representantes indicados para as visitas deverão comparecer à recepção da FAPEMIG, no endereço Av. José Cândido da Silveira, N° 1.500, Horto - CEP: 31035-536 - Belo Horizonte/MG, no dia e horário escolhido, com tolerância de atraso de até 15 (quinze) minutos.

III. A vistoria técnica será acompanhada pelo servidor: Flávio Henrique Belo Rodrigues;

IV. Alegações posteriores relacionadas com o desconhecimento de condições locais, ou de projetos ou amostras porventura disponibilizadas, se for o caso, não serão consideradas para reclamações futuras, ou de forma a desobrigar a sua execução;

15. Da subcontratação

A subcontratação limitar-se-á à contratação de mão-de-obra ou serviço especializado de assistência técnica e manutenção dos equipamentos da infraestrutura de rede atual da FAPEMIG e locação, assistência técnica e manutenção de nobreaks e gerador, não superior a 10% (dez por cento) do valor total do contrato.

Caso os serviços de assistência técnica e manutenção sejam de responsabilidade de terceiro, a CONTRATADA será solidariamente responsável por eles, respondendo, portanto, por eventuais falhas, defeitos ou danos decorrentes da mencionada prestação de serviços.

É de responsabilidade da contratada identificar os subcontratados, garantir que possuam experiência e as credenciais necessárias para desempenhar a atividade subcontratada, que atendam aos requisitos aqui estabelecidos e que estejam qualificados para atender o nível de serviço e demais exigências especificadas neste documento.

Todos os atestados, laudos e certificados exigidos na licitação, e também para a contratação, deverão ser apresentados pelo licitante.

Não serão aceitos atestados, laudos e certificados emitidos em nome de empresa subcontratada.

A subcontratação não exime o licitante, tampouco o contratado, das obrigações e responsabilidades decorrentes da licitação e da contratação.

16. Obrigações específicas das partes

16.1. Da contratada

I. Prestar os serviços nas quantidades, prazos e condições pactuadas, de acordo com as exigências constantes neste documento;

II. Emitir faturas no valor pactuado, apresentando-as ao CONTRATANTE para ateste e pagamento;

III. Atender prontamente as orientações e exigências inerentes à execução do objeto contratado;

IV. Assegurar ao CONTRATANTE o direito de sustar, recusar, mandar desfazer ou refazer qualquer serviço/produto que não esteja de acordo com as normas e especificações técnicas recomendadas neste documento;

V. Assumir inteira responsabilidade pela entrega dos materiais, responsabilizando-se pelo transporte, acondicionamento e descarregamento dos materiais;

VI. Responsabilizar-se pela garantia dos materiais empregados nos itens solicitados, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme previsto na legislação em vigor e na forma exigida neste termo de referência;

VII. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do objeto deste Termo de Referência;

VIII. Não transferir para o CONTRATANTE a responsabilidade pelo pagamento dos encargos estabelecidos no item anterior, quando houver inadimplência da CONTRATADA, nem onerar o objeto deste Termo de Referência;

IX. Manter, durante toda a execução do objeto, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

X. Manter preposto, aceito pela Administração, para representá-lo na execução do objeto contratado;

XI. Responder pelos danos causados diretamente à CONTRATANTE ou aos seus bens, ou ainda a terceiros, decorrentes de sua culpa ou dolo na execução do objeto;

XII. Em nenhuma hipótese a FAPEMIG poderá ser responsabilizada pelos serviços executados pela contratada, bem como pelos seus funcionários e quaisquer de suas obrigações trabalhistas.

16.2. Da contratante

I. Acompanhar e fiscalizar os serviços, atestar nas notas fiscais/faturas o efetivo fornecimento do objeto deste Termo de Referência;

II. Rejeitar, no todo ou em parte os itens entregues, se estiverem em desacordo com a especificação e da proposta de preços da CONTRATADA;

III. Comunicar a CONTRATADA todas as irregularidades observadas durante o recebimento dos itens solicitados;

IV. Notificar a CONTRATADA no caso de irregularidades encontradas na entrega dos itens solicitados;

V. Solicitar o reparo, a correção, a remoção ou a substituição dos materiais/serviços em que se verificarem vícios, defeitos ou incorreções;

VI. Conceder prazo de 03 (três) dias úteis, após a notificação, para a CONTRATADA regularizar as falhas observadas;

VII. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

VIII. Aplicar à CONTRATADA as sanções regulamentares;

IX. Exigir o cumprimento dos recolhimentos tributários, trabalhistas e previdenciários através dos documentos pertinentes;

X. Disponibilizar local adequado para a realização do serviço.

17. Sanções administrativas

I. A CONTRATADA que cometer qualquer das infrações, previstas na Lei Federal nº 8.666, de 21 de junho de 1993, na Lei Federal nº 10.520, de 17 de julho de 2002, Lei Estadual n.º 14.167, de 10 de janeiro de 2002 e no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a. advertência por escrito;

b. multa de até:

i. 0,3 % (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do objeto não executado;

ii. 10% (dez por cento) sobre o valor da nota de empenho ou do contrato, em caso de recusa do adjudicatário em efetuar o reforço

de garantia de execução exigida; (retirar caso não haja garantia de execução);

iii. 20% (vinte por cento) sobre o valor da prestação de serviços após ultrapassado o prazo de 30 dias de atraso, ou no caso de não entrega do objeto, ou entrega com vícios ou defeitos ocultos que o torne impróprio ao uso a que é destinado, ou diminua-lhe o valor ou, ainda fora das especificações contratadas;

iv. 2% (dois por cento) sobre o valor total do contrato, em caso de descumprimento das demais obrigações contratuais ou norma da legislação pertinente.

c. Suspensão do direito de participar de licitações e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos;

d. Impedimento de licitar e contratar com a Administração Pública Estadual, nos termos do art. 7º da lei 10.520, de 2002;

e. Declaração de inidoneidade para licitar ou contratar com a Administração Pública;

II. A sanção de multa poderá ser aplicada cumulativamente às demais sanções previstas nos itens 17.I.a, 17.I.b, 17.I.d, 17.I.e.

III. A multa será descontada da garantia do contrato, quando houver, e/ou de pagamentos eventualmente devidos pelo INFRATOR e/ou cobrada administrativa e/ou judicialmente.

IV. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo incidental apensado ao processo licitatório ou ao processo de execução contratual originário que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto no Decreto Estadual nº. 45.902, de 27 de janeiro de 2012, bem como o disposto na Lei 8.666, de 1993 e Lei Estadual nº 14.184, de 2002.

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

a. Não serão aplicadas sanções administrativas na ocorrência de casos fortuitos, força maior ou razões de interesse público, devidamente comprovados.

VI. A aplicação de sanções administrativas não reduz nem isenta a obrigação da CONTRATADA de indenizar integralmente eventuais danos causados a

Administração ou a terceiros, que poderão ser apurados no mesmo processo administrativo sancionatório.

VII. As sanções relacionadas nos itens 17.I.c, 17.I.d e 17.I.e serão obrigatoriamente registradas no Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual – CAFIMP.

VIII. As sanções de suspensão do direito de participar em licitações e impedimento de licitar e contratar com a Administração Pública poderão ser também aplicadas àqueles que:

a. Retardarem a execução do objeto;

b. Comportar-se de modo inidôneo;

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

c. Apresentarem documentação falsa ou cometerem fraude fiscal.

IX. Durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei Federal nº 12.846, de 2013, e pelo Decreto Estadual nº 46.782, de 2015, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à Controladoria-Geral do Estado, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

ANEXO II – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE MONITORAMENTO E GERENCIAMENTO

Item	Característica
1	A solução deverá ser configurada com licença para gerenciamento de número ilimitado de dispositivos ou todas as licenças necessárias para atendimento a demanda, incluindo novos itens de configuração que venham a ser incorporados à Rede FAPEMIG.
2	Deve prover interface de gerenciamento através dos protocolos HTTP e HTTPS compatível com os browsers padrões de mercado, como Microsoft IE versão 6 ou superior e Mozilla Firefox versão 3 ou superior.
3	Deve permitir a configuração e o gerenciamento de Vlans de forma centralizada.
4	Deve permitir a configuração e o gerenciamento de ACLs de forma centralizada.
5	Deve possibilitar o gerenciamento através de SNMP v3, 4 grupos de RMON (caso o equipamento gerenciado suporte os 4 grupos) e scripts de configuração.
6	Deve permitir atualização de firmware dos produtos ofertados.
7	Deve permitir realizar backups/restore das configurações dos elementos de rede.
8	Deve receber as notificações via traps SNMP e mensagens Syslog permitindo buscas por dispositivo de origem e severidade da mensagem.
9	Deve possibilitar a notificação de eventos através de e-mail.
10	Deve permitir a geração de relatórios gráficos ou visualização na tela de gerência de estatísticas de utilização por portas, por MAC addresses, por IP, por aplicação, ou por usuários 802.1x
11	Deve exibir os mapas da rede de forma gráfica permitindo a visualização da rede por topologias de IP e de Vlans.
12	Deve possuir a facilidade de "auto discovery" de elementos de rede.
13	Deve suportar perfis de usuários com níveis de privilégio diferentes suportando ao menos usuários para somente leitura, leitura e escrita.
14	Deve suportar regiões administrativas permitindo o acesso ao gerente a um número restrito de equipamentos.

Item	Característica
15	Deve permitir o gerenciamento de todos os agentes SNMP dos dispositivos que compõe a infraestrutura de TI;
16	Deve permitir o descobrimento de equipamentos presentes em uma ou mais sub-redes, a fim de garantir uma auditoria constante na infraestrutura de TI; Deve permitir a criação de topologias / mapas automáticos da rede através de protocolos Layer 2. O mapa deve permitir a identificação de problemas com os dispositivos visualmente; Permitir a visão agrupada da topologia conforme configuração do usuário.
17	Deve permitir o gerenciamento das configurações de filas e priorização de tráfego dos dispositivos da rede.
18	Deve permitir a criação e o gerenciamento de políticas de acesso à rede nos dispositivos.
19	O software deve permitir a criação, edição, remoção de VLANs nos dispositivos e associação das portas as mesmas.
20	A solução deve permitir o inventário detalhado de atributos dos dispositivos da rede, atendendo no mínimo: hostname, ip, números seriais, part number, marca, modelo, localização, versão de firmware, tipo de CPU e memória.
21	A solução deve permitir o armazenamento histórico das configurações dos dispositivos e permitir a comparação da configuração atual com a configuração armazenada.
22	A solução deve possuir a capacidade de gerar relatórios para planejamento de capacidade, atendendo no mínimo a geração de relatórios da utilização mínima de chassis e portas.
23	Acesso completo a partir das estações de trabalho da CONTRATANTE (até 03 acessos simultâneos)

ANEXO III – ESPECIFICAÇÕES DOS ATIVOS DE REDE

1. SWITCH CORE

Grupo	Item	Descrição	Especificação Mínima
Capacidade e desempenho	CD1	Todas as interfaces deverão operar a plena carga, obedecendo no mínimo a taxa de comunicação entre os slots de módulos de interface, full-duplex conforme item CD6. Vale ressaltar que estrangulamentos serão permitidos somente de acordo com a própria topologia da solução.	Obrigatório
	CD2	Capacidade de backplane.	1 Tbps
	CD3	Taxa de encaminhamento de pacotes, considerando pacotes de 64 Bytes, nas camadas 2 e 3, em sua configuração máxima.	400 Mbps
	CD4	Processamento de pacotes nas camadas 2 e 3 utilizando arquitetura distribuída. O processamento ou encaminhamento dos pacotes de IPv4 e/ou IPv6 devem ser realizados nos módulos de I/O, e não em um módulo de supervisão ou módulo de Switch Fabric centralizado, mantendo o gerenciamento desta distribuição baseado nos módulos de gerenciamento.	Obrigatório
	CD5	Capacidade de armazenamento de endereços MAC.	60000
	CD6	Taxa de comunicação entre os slots de módulos de interface, full-duplex: 40 Gbps - placas 48p 20 Gbps - placas 24p	Obrigatório
	CD6	Capacidade de suporte de rotas entradas IP, em hardware.	45000
	CD7	Capacidade de suporte de VRF "Virtual Routing and Forwarding".	60
	CD8	Suporte a IPv6 em hardware	Obrigatório
	CD9	Suporte a VLAN´s	1000
	CD10	Possibilitar a adição de entradas estáticas à tabela de endereços MAC do switch.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	CD11	Deve suportar configuração de alta disponibilidade, permitindo conexões com os equipamentos de acesso sem utilização do protocolo spanning tree. (Lembrando que a topologia obriga que os switchs de distribuição estejam interligados).	Obrigatório
	CD12	Deve suportar Jumbo Frames.	Obrigatório
	CD13	Implementar controle de Broadcast permitindo fixar o limite máximo de pacotes por porta.	Obrigatório
Interfaces	IT1	Portas Gigabit Ethernet 1000BASE-T Full Duplex, Autosense, suportando taxas de 10/100/1000 Mbps com autonegociação, com conector RJ45 Cat 6.	48
	IT2	14 Gigabit Ethernet removíveis (tipo Xenpak, XFP, SFP+ ou X2) 10000-Base-SR (multimodo).	Interface-pontos
	IT3	Capacidade de adição de interfaces 10 Gigabit.	Quantidade: 4
Alta disponibilidade	AD1	Todos os módulos devem ser hot-swappable.	Obrigatório
	AD2	Em caso de falha nos módulos de Supervisão, gerência ou Switch Fabric, não deve haver degradação de performance e o tempo de indisponibilidade da rede deve ser da ordem de unidades segundos.	Obrigatório
	AD3	Deve ser fornecido com fontes de alimentação internas AC bi volt, com seleção automática de voltagem, de 110/220V 60Hz, em configuração de redundância tipo N+N ou N+1, hotswappable, load-sharing, com cabos de alimentação independentes.	Obrigatório
	AD4	Deve possuir sistema de ventilação redundante através de duas placas ou através de redundância de ventiladores na mesma placa.	Obrigatório
	AD5	Deve permitir aplicação de patches de correção de software de sistema operacional do equipamento sem impacto na rede.	Obrigatório
	AD6	Deve implementar a RFC 3623 - Graceful OSPF Restart.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	AD7	Deve implementar RFC 3768 VRRP.	Obrigatório
Qualidade de Serviços	QS1	Deve implementar as seguintes normas IEEE e RFCs: – RFC 2475 An Architecture for Differentiated Services (Diffserv) ou – RFC 2474 Definition of the Differentiated Services Field (DS Field)".	Obrigatório
	QS2	Possibilitar a implementação simultânea de ao menos 1 método de processamento de filas em uma mesma porta.	1 método
	QS3	Implementar no mínimo um dos seguintes algoritmos de tratamento das filas de prioridade: -Weighted fair queuing (WFQ) -Class based weighted fair queuing -Weighted round robin (WRR) -Deficit weighted round robin (DWRR) -Hierarchical Fair Service Curve (HFSC) -Strict Priority (SP)	1 ao menos
	QS4	Implementar filas para priorização de tráfego por porta 10G Ethernet.	8 filas
Segurança	SE1	Possuir capacidade de criação de ACLs (Access Control List) em Hardware com performance "Wire-Speed".	Obrigatório
	SE2	Deve permitir a criação de filtros ou Access Control Lists (ACLs) usando endereços IP ou MAC de origem e destino, e portas TCP ou UDP de origem e destino.	Obrigatório
	SE3	O equipamento proposto deve possuir mecanismos para proteção contra-ataques do tipo "Denial of Service".	Obrigatório
	SE4	Deve suportar autenticação de acesso ao switch através de RADIUS ou TACACS+.	Obrigatório
	SE5	Deve implementar mecanismo anti-ataque do tipo IP spoofing.	Obrigatório
Gerência	GE1	Deve suportar portas para monitoração ou espelhamento (PORT MIRRORING), para uso com	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
		analisadores de protocolo ou serviços de IDS (Intrusion Detection Systems).	
	GE2	Deve permitir a atualização de imagens de firmware, upload e download dos arquivos de configuração usando os protocolos TFTP ou FTP.	Obrigatório
	GE3	Deve possuir porta de console para manutenção, configuração e administração, sendo fornecido com todos os cabos necessários para conexão e implementar gerenciamento através de Telnet e SSH v.2.	Obrigatório
	GE4	Deve permitir a geração syslog para gerenciamento remoto.	Obrigatório
	GE5	O fabricante deve fornecer os arquivos da biblioteca MIB (MIB II, Bridge MIB e RMON MIB) para gerência do equipamento proposto.	Obrigatório
	GE6	Possuir suporte para gerenciamento SNMP(v1, v2 ou v2c e v3) e ao menos 2 grupos de RMON, sem adição de probes externas.	Obrigatório
	GE7	O Chassi deve ser fornecido com todo o Hardware e Software necessários para disponibilização, por parte do Switch, de recursos de "Análise de Rede" e "Serviços de Monitoração de Tráfego" em todas as portas, utilizando a tecnologia NETFLOW (versão 5 ou 9) ou, alternativamente, SFLOW (IETF RFC3176). Outras tecnologias de monitoração (proprietárias) não serão aceitas	Obrigatório
	GE8	Os equipamentos propostos devem acompanhar hardware e software centralizado - incluindo licenças de Sistema Operacional se necessário, para coleta de estatísticas geradas pelo protocolo NETFLOW ou SFLOW, compatível com o equipamento ofertado, oferecendo análise do tráfego com pelo menos as informações de: consumo por aplicação e por endereços de	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
		origem/destino, e fornecendo visualização via http e https, em forma de gráficos.	
	GE9	Deve suportar o software de gerenciamento, cuja especificação faz parte deste edital.	Obrigatório
	GE10	Suportar ajuste de hora através do protocolo NTP ou SNTP.	Obrigatório
Padronização	PA1	Deve implementar roteamento dinâmico OSPF e BGP4; ● IEEE 802.1Q VLAN encapsulation ● Support for up to 4096 VLANs ● Rapid Per-VLAN Spanning Tree Plus (PVRST+) (IEEE 802.1w compatible) ● MSTP (IEEE 802.1s): 64 instances ● LACP: IEEE 802.3ad, IEEE 802.1ax ● Jumbo frames on all ports ● Storm control (multicast and broadcast) ● Link-level flow control (IEEE 802.3x)	Obrigatório
	PA2	Demais formas de roteamento exigidas: - Roteamento estático - RIP v1 e v2	Obrigatório
	PA3	IEEE 802.1D (STP)	Obrigatório
	PA4	IEEE 802.1p (COS)	Obrigatório
	PA5	IEEE 802.1Q (VLAN)	Obrigatório
	PA6	IEEE 802.1s (MSTP)	Obrigatório
	PA7	IEEE 802.1w (RSTP)	Obrigatório
	PA9	IEEE 802.3ab (1000BASE-T)	Obrigatório
	PA10	IEEE 802.3ad (Link aggregation)	Obrigatório
	PA11	IEEE 802.3ae (10GBASE-X)	Obrigatório
	PA12	IEEE 802.1ax: Link Aggregation Control Protocol (LACP)	Obrigatório
	PA13	IEEE 802.3ba: 40 Gigabit Ethernet	Obrigatório
	PA14	IEEE 802.3x (Flow control)	Obrigatório
	PA15	IEEE 802.3z (Gigabit)	Obrigatório
	PA16	PA RFC 768 (UDP)	Obrigatório
	PA17	RFC 791 (IP)	Obrigatório
	PA18	RFC 792 ou 950 (ICMP)	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	PA19	RFC 793 (TCP)	Obrigatório
	PA20	RFC 826 (ARP)	Obrigatório
	PA21	RFC 951 (BOOTP)	Obrigatório
	PA22	RFC 1122 (IP Host Requirements	Obrigatório
	PA23	RFC 1518 ou1519 (CIDR)	Obrigatório
	PA24	RFC 1542 (BOOTP)	Obrigatório
	PA25	RFC 1723 ou 2453 (RIP v2)	Obrigatório
	PA26	RFC 1812 ou 2644 (IPv4)	Obrigatório
	PA27	RFC 1997 ou 1998 (BGP Communities)	Obrigatório
	PA28	RFC 2131 ou 3396 (DHCP)	Obrigatório
	PA29	RFC 2236 (IGMP v2)	Obrigatório
	PA30	RFC 2328 (OSPF v2)	Obrigatório
	PA31	RFC 2338 ou 3768 (VRRP)	Obrigatório
	PA32	RFC 2370 ou 3630 (OSPF Opaque LSA option)	Obrigatório
	PA33	RFC 2385 (BGP – MD5)	Obrigatório
	PA34	RFC 2439 (BGP Route flap dampening)	Obrigatório
	PA35	RFC 2475 (Architecture for Diffserv) ou 2474.	Obrigatório
	PA36	RFC 2796 (BGP Route reflection) ou RFC 4456	Obrigatório
	PA37	RFC 2918 (BGP-4 Route Refresh)	Obrigatório
	PA38	RFC 3065 (BGP AS)	Obrigatório
	PA39	RFC 3101 (OSPF NSSA)	Obrigatório
	PA40	RFC 3376 (IGMP v3)	Obrigatório
	PA41	RFC 3392 (BGP Capabilities Advertisement)	Obrigatório
	PA42	RFC 3768 ou 2338 (VRRP)	Obrigatório
Condições operacionais	AE1	Alimentação (tensão).	220 VAC
	AE2	Alimentação / frequência.	60 Hz

2. SWITCH DE DESTRIBUIÇÃO (LAYER 3)

Subitem		Característica	Especificação	Exigência
Conexões	1.1	Portas RJ-45	24 (vinte e quatro) portas Gigabit Ethernet 1000Base-T padrão IEEE 802.3ab, full-duplex, auto negociável, auto sensing, com conectores RJ-45 tipo fêmea, compatível com Fast Ethernet 100Base-TX padrão IEEE 802.3u.	Mínimo Obrigatório
	1.2	Portas GBIC	Mínimo 4 (Quatro) portas 10 Gigabit Ethernet padrão IEEE 802.3ae, para inserção de transceivers do tipo SFP+ ou XFP. Deverão ser fornecidos 4 (quatro) adaptadores mini-GBIC SFP+ 10GBASE-SR padrão 802.3ae compatíveis os slots SFP+ ou XFP presentes no equipamento. Cada adaptador deverá possuir conexão para fibra óptica padrão ISO/IEC 11801 OM3 (multimodo) com conector SC ou LC ou MT RJ, e acompanhar cordão óptico de comprimento mínimo de 1,5m compatível para ligação a conector SC.	Mínimo Obrigatório
	1.3	Autoconfiguração	Implementação de mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X.	Obrigatório
	1.4	Console	1 (uma) porta console para ligação direta e acesso através de terminal de linha de comando, para conexão com interface DB-9 ou USB ou RJ-45.	Mínimo Obrigatório

Subitem		Característica	Especificação	Exigência
	1.5	Empilhamento	Permitir o empilhamento de até 8 equipamentos do mesmo modelo por caminhos redundantes (daisy-chain/closed-loop), de forma a utilizar uma única interface e IP de gerenciamento. As portas de empilhamento devem ser adicionais às solicitadas nos subitens 1.1 a 1.4.	Mínimo Obrigatório
	1.6	Indicadores de status portas	LEDs ou dispositivo de função equivalente para indicação do status de cada porta.	Mínimo Obrigatório
Desempenho	2.1	Agregação de Links	Agregação de links segundo o padrão IEEE 802.3ad. Deve implementar no mínimo até 6 grupos de até 8 portas.	Mínimo Obrigatório
	2.2	Vazão (throughput)	Capacidade de comutação de no mínimo 108 Gbps non-blocking.	Mínimo Obrigatório
	2.3	Repasse (forwarding)	Capacidade de encaminhamento de pacotes de no mínimo 74 Mpps non-blocking, considerando pacotes de 64 bytes.	Mínimo Obrigatório
	2.4	MACs	Suportar armazenamento de 16.000 endereços MAC .	Mínimo Obrigatório
	2.5	VLANs IDs	Implementar a configuração de 12 VLANs IDs.	Mínimo Obrigatório
	2.6	VLANs	Implementar redes virtuais (VLAN), dentro do padrão IEEE 802.1Q.	Mínimo Obrigatório
Funcionalidades	3.1	Padrões / Funcionalidades	IEEE 802.1d – Protocolo Spanning Tree.	Obrigatório
	3.2		IEEE 802.1w – Protocolo Rapid Spanning Tree.	Obrigatório
	3.3		IEEE 802.1s – Protocolo Multiple Spanning Tree.	Obrigatório

Subitem		Característica	Especificação	Exigência
	3.4		IEEE 802.3x – Controle de Fluxo	Obrigatório
	3.5		IEEE 802.3ad – Agregação de links	Obrigatório
	3.6		IEEE 802.1x – Controle de Acesso à Rede	Obrigatório
	3.7		IEEE 802.1p – CoS – Classe de Serviço (Class of Service)	Obrigatório
	3.8		Implementar proteção de BPDU (Blocks Bridge Protocol Data Units).	Obrigatório
	3.9		Implementar mecanismos que possibilitem a limitação e controle de broadcast.	Obrigatório
	3.10		Implementar IGMP snooping.	Obrigatório
	3.11		Implementar mecanismos de proteção contra ARP spoofing.	Obrigatório
	3.12		DHCP snooping ou mecanismos similares que permitam o bloqueio de servidores DHCP não autorizados.	Obrigatório
	3.13		Implementar os protocolos LLDP (IEEE 802.1ab) e LLDP-MED (ANSI/TIA-1057)	Obrigatório
	3.14		Encaminhamento de Jumbo Frames de no mínimo 9.000 bytes nas portas Gigabit Ethernet.	Obrigatório
	3.15		Implementar a capacidade automática de reconhecer telefones IP e configurá-los na VLAN de voz.	Obrigatório
	3.16		Implementar IPv6, inclusive para as interfaces de gerenciamento.	Obrigatório
	3.17		Implementar ICMPv6 (RFC 4443).	Obrigatório

Subitem		Característica	Especificação	Exigência
Funcionalidades Camada 3	4.1	Funcionalidades	Implementar rotas estáticas.	Obrigatório
	4.2		Implementar redistribuição de rotas entre protocolos.	Obrigatório
	4.3		Implementar geração de logs dos protocolos.	Obrigatório
	4.4		Implementar e suportar RFC2338 ou RFC 3768 – VRRP para IPv4 (Virtual Router Redundancy Protocol) ou funcionalidade similar.	Obrigatório
	4.5	Protocolos	RFC 1723 ou RFC 2453 (RIPv2).	Obrigatório
	4.6		RFC 2328 (OSPFv2).	Obrigatório
	4.7		RFC 1587 ou RFC 3101 (OSPF NSSA).	Obrigatório
	4.8		8 áreas OSPFv2.	Mínimo Obrigatório
	4.9		15 adjacências OSPFv2.	Mínimo Obrigatório
	4.10		Implementar autenticação via "simple-password" e/ou "MD5".	Obrigatório
	4.11		OSPFv3.	Obrigatório
Gerenciamento	5.1		Implementar os protocolos SNMPv2c e SNMPv3, com capacidade de monitoração de no mínimo: tráfego de interfaces, uso de CPU e uso de memória.	Mínimo Obrigatório
	5.2		Implementar RMON.	Obrigatório
	5.3		Implementar MIB II (RFC 1213).	Mínimo Obrigatório
	5.4		Implementar espelhamento de tráfego de entrada e saída de múltiplas portas em uma única porta.	Obrigatório
	5.5		Implementar espelhamento de tráfego de entrada e saída de	Obrigatório

Subitem		Característica	Especificação	Exigência
			múltiplas VLANs em uma única porta.	
	5.6		Implementar configuração através de TELNET.	Obrigatório
	5.7		Implementar configuração através de SSHv2.	Obrigatório
	5.8		Implementar gerenciamento via interface web HTTPS.	Obrigatório
	5.9		Implementar FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol) ou SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol).	Mínimo Obrigatório
	5.10		Implementar NTP (Network Time Protocol), ou SNTP (Simple Network Time Protocol).	Obrigatório
	5.11		Implementar Syslog.	Obrigatório
	5.12		Os utilitários e protocolos de gerenciamento devem ser implementados sobre IPv6 (ping, traceroute, Telnet, SNMP).	Obrigatório
	5.13		Implementar múltiplas imagens de firmware ou permitir a atualização da imagem por intermédio de download de servidor de rede.	Obrigatório
	5.14		Permitir o download e upload de arquivo de configurações.	Obrigatório
Segurança	6.1	Autenticação e Controle	IEEE 802.1x - Controle de acesso por porta, com configuração dinâmica da VLAN do usuário autenticado.	Obrigatório
	6.2		Implementar os protocolos RADIUS e TACACS+ .	Obrigatório

Subitem		Característica	Especificação	Exigência
	6.3		Deve implementar filtros de ACL, permitindo a elaboração de regras.	Obrigatório
	6.4		Implementar grupos de usuários com diferentes níveis de acesso, ou possuir pelo menos 3 grupos de usuários pré-definidos. Deverá possuir um controle de comandos para usuários ou grupos no equipamento.	Obrigatório
	6.5		Implementar Private VLAN ou funcionalidade similar que permita segmentar uma VLAN em subdomínios: uma VLAN primária e múltiplas VLANs secundárias.	Obrigatório
	6.6		O equipamento deve incluir proteção contra-ataques de negação de serviço (denial of service).	Obrigatório
	6.7		O equipamento deve prover mecanismos de detecção e supressão de ataques do tipo ARP.	Obrigatório
Qualidade de serviço	7.1		Implementar Qualidade de Serviço (QoS), de acordo com o padrão IEEE 802.1p (priorização de tráfego por porta).	Mínimo Obrigatório
	7.2		Deverá implementar no mínimo 7 (sete) filas de QoS por porta baseada em hardware.	Mínimo Obrigatório
	7.3		Implementar Qualidade de Serviço (QoS) de acordo com a RFC 2474, ou RFC 2475 (An Architecture for Differentiated Service), ou equivalente.	Mínimo Obrigatório

Subitem		Característica	Especificação	Exigência
	7.4		Implementar os algoritmos de gerenciamento de filas: Deficit Weighted Round Robin (DWRR), ou Weighted Round Robin (WRR), ou Deficit Round Robin (DRR), ou Weighted Fair Queuing (WFQ) e Strict Priority (SP), ou Weighted Tail-Drop (WTD) como mecanismo de prevenção de congestionamento.	Mínimo Obrigatório
	7.5		Implementar classificação e marcação de pacotes baseada em CoS (Class of Service) padrão IEEE 802.1p.	Obrigatório
	7.6		Implementar classificação e marcação de pacotes baseada em marcação DSCP.	Obrigatório
	7.7		Implementar classificação e marcação de pacotes baseada em: endereço de origem, porta de origem, endereço de destino, porta de destino.	Obrigatório
Demais condições	8.1	Certificado	Possuir homologação da ANATEL, de acordo com a resolução número 242 de 30/11/2000.	Obrigatório
	8.2	Firmware	A versão da placa (ou módulo) de gerenciamento, ou de qualquer outro módulo existente no equipamento, e seus respectivos programas de controle (on-board ou não) deverão ser os mais atuais existentes no momento da entrega do equipamento.	Obrigatório

Subitem		Característica	Especificação	Exigência
	8.3		Novas versões e/ou patches dos softwares integrantes da solução ofertada (on-board ou não) dos módulos do equipamento deverão ser fornecidas gratuitamente durante o período de garantia. Estas versões deverão ser fornecidas pelo fabricante num período máximo de 60 (sessenta) dias após sua divulgação no mercado, devendo a CONTRATADA prestar suporte técnico telefônico para o procedimento de atualização.	Obrigatório
	8.4		A cada atualização realizada deverão ser fornecidos os manuais técnicos originais e documentos comprobatórios do licenciamento da nova versão/patch.	Obrigatório
Características físicas	9.1		Deve possuir fonte de alimentação com capacidade de operar em tensões de 100 a 240 V e em frequências de 50/60 Hz.	Mínimo Obrigatório
	9.2		O equipamento será destinado ao uso em ambiente com umidade relativa na faixa de 20 a 80% (sem condensação) e temperatura ambiente na faixa de 5 a 40 °C.	Mínimo Obrigatório
	9.3		O equipamento deverá vir acompanhado de cabos de força, acessórios e cabo de acesso a console do equipamento para configuração do mesmo.	Mínimo Obrigatório

Subitem		Característica	Especificação	Exigência
	9.4		O equipamento deverá vir acompanhado de todos os módulos e/ou dispositivos necessários para seu perfeito funcionamento e operação, em conformidade com as especificações técnicas aqui apresentadas, mesmo que esses não constem desta especificação.	Mínimo Obrigatório
	9.5		O equipamento deverá possuir manual de todos os dispositivos e softwares que acompanham o conjunto. Toda documentação – manuais, guia de usuário, recomendações, etc., deverá ser fornecida em papel ou mídia magnética (formato PDF ou CHM), em língua portuguesa ou inglesa.	Obrigatório

3. SWITCH DE ACESSO (LAYER 2)

Subitem		Característica	Especificação	Exigências
Conexões	1.1	Portas RJ-45	24 (vinte e quatro) portas Gigabit Ethernet 1000Base-T padrão IEEE 802.3ab, full-duplex, auto negociável, auto sensing, com conectores RJ-45 tipo fêmea, compatível com Fast Ethernet 100Base-TX padrão IEEE 802.3u.	Mínimo Obrigatório
	1.2	PoE	Implementar o padrão IEEE 802.3af (PoE) nas portas do subitem 1.1, alimentando todas as portas na potência de 15,4 W	Mínimo Obrigatório

Subitem		Característica	Especificação	Exigências
			sem necessidade de fonte externa.	
	1.3	PoE+	Implementar o padrão IEEE 802.3at (PoE+) nas portas do subitem 1.1. Deverá permitir a habilitação da funcionalidade em, no mínimo, 5 portas, sem a necessidade de fonte externa.	Mínimo Obrigatório
	1.4	Portas GBIC	Mínimo 2 (duas) portas 10 Gigabit Ethernet padrão IEEE 802.3ae, para inserção de transceivers do tipo SFP+.	Mínimo Obrigatório
			Deverão ser fornecidos 2 (dois) adaptadores mini-GBIC SFP+ 10GBASE-SR padrão 802.3ae compatíveis com os slots SFP+ presentes no equipamento. Cada adaptador deverá possuir conexão para fibra óptica padrão ISO/IEC 11801 OM3 (multimodo) com conector SC ou LC ou MT RJ, e acompanhar cordão óptico de comprimento mínimo de 1,5m compatível para ligação a conector SC.	
	1.5	Autoconfiguração	Implementação de mecanismos de autoconfiguração em todas as portas, do tipo MDI/MDI-X.	Obrigatório
	1.6	Console	1 (uma) porta console para ligação direta e acesso através de terminal de linha de comando, para conexão com interface DB-9 ou USB ou RJ-45.	Mínimo Obrigatório

Subitem		Característica	Especificação	Exigências
	1.7	Empilhamento	Permitir o empilhamento de até 4 equipamentos do mesmo modelo por caminhos redundantes (daisy-chain/closed-loop), de forma a utilizar uma única interface e IP de gerenciamento. As portas de empilhamento devem ser adicionais às solicitadas nos subitens 1.1 a 1.6.	Mínimo Obrigatório
	1.8	Indicadores de status portas	LEDs ou dispositivo de função equivalente para indicação do status de cada porta.	Mínimo Obrigatório
Desempenho	2.1	Agregação de Links	Agregação de links segundo o padrão IEEE 802.3ad. Deve implementar no mínimo até 6 grupos de até 8 portas.	Mínimo Obrigatório
	2.2	Vazão (throughput)	Capacidade de comutação de no mínimo 108 Gbps non-blocking.	Mínimo Obrigatório
	2.3	Repasse (forwarding)	Capacidade de encaminhamento de pacotes de no mínimo 74 Mpps non-blocking, considerando pacotes de 64 bytes.	Mínimo Obrigatório
	2.4	MACs	Suportar armazenamento de 16.000 endereços MAC.	Mínimo Obrigatório
	2.5	VLANs IDs	Implementar a configuração de 12 VLANs IDs.	Mínimo Obrigatório
	2.6	VLANs	Implementar redes virtuais (VLAN), dentro do padrão IEEE 802.1Q.	Mínimo Obrigatório
Funcionalidades	3.1	Padrões / Funcionalidades	IEEE 802.1d – Protocolo Spanning Tree.	Obrigatório
	3.2		IEEE 802.1w – Protocolo Rapid Spanning Tree.	Obrigatório
	3.3		IEEE 802.1s – Protocolo Multiple Spanning Tree.	Obrigatório
	3.4		IEEE 802.3x – Controle de Fluxo	Obrigatório

Subitem		Característica	Especificação	Exigências
	3.5		IEEE 802.3ad – Agregação de links	Obrigatório
	3.6		IEEE 802.1x – Controle de Acesso à Rede	Obrigatório
	3.7		IEEE 802.1p – CoS – Classe de Serviço (Class of Service)	Obrigatório
	3.8		Implementar proteção de BPDU (Blocks Bridge Protocol Data Units).	Obrigatório
	3.9		Implementar mecanismos que possibilitem a limitação e controle de broadcast.	Obrigatório
	3.10		Implementar IGMP snooping.	Obrigatório
	3.11		Implementar mecanismos de proteção contra ARP spoofing.	Obrigatório
	3.12		DHCP snooping ou mecanismos similares que permitam o bloqueio de servidores DHCP não autorizados.	Obrigatório
	3.13		Implementar os protocolos LLDP (IEEE 802.1ab) e LLDP-MED (ANSI/TIA-1057)	Obrigatório
	3.14		Encaminhamento de Jumbo Frames de no mínimo 9.000 bytes nas portas Gigabit Ethernet.	Obrigatório
	3.15		Implementar a capacidade automática de reconhecer telefones IP e configurá-los na VLAN de voz.	Obrigatório
	3.16		Implementar IPv6, inclusive para as interfaces de gerenciamento.	Obrigatório
	3.17		Implementar ICMPv6 (RFC 4443)	Obrigatório
Gerenciamento	4.1		Implementar os protocolos SNMPv2c e SNMPv3, com capacidade de monitoração de no	Mínimo Obrigatório

Subitem		Característica	Especificação	Exigências
			mínimo: tráfego de interfaces, uso de CPU e uso de memória.	
	4.2		Implementar RMON.	Obrigatório
	4.3		Implementar MIB II (RFC 1213).	Mínimo Obrigatório
	4.4		Implementar espelhamento de tráfego de entrada e saída de múltiplas portas em uma única porta.	Obrigatório
	4.5		Implementar espelhamento de tráfego de entrada e saída de múltiplas VLANs em uma única porta.	Obrigatório
	4.6		Implementar configuração através de TELNET.	Obrigatório
	4.7		Implementar configuração através de SSHv2.	Obrigatório
	4.8		Implementar gerenciamento via interface web HTTPS.	Obrigatório
	4.9		Implementar FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol) ou SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol).	Mínimo Obrigatório
	4.10		Implementar NTP (Network Time Protocol), ou SNTP (Simple Network Time Protocol).	Obrigatório
	4.11		Implementar Syslog.	Obrigatório
	4.12		Os utilitários e protocolos de gerenciamento devem ser implementados sobre IPv6 (ping, traceroute, Telnet, SNMP).	Obrigatório
	4.13		Implementar múltiplas imagens de firmware ou permitir a	Obrigatório

Subitem		Característica	Especificação	Exigências
			atualização da imagem por intermédio de download de servidor de rede.	
	4.14		Permitir o download e upload de arquivo de configurações.	Obrigatório
Segurança	5.1	Autenticação e Controle	IEEE 802.1x - Controle de acesso por porta, com configuração dinâmica da VLAN do usuário autenticado.	Obrigatório
	5.2		Implementar os protocolos RADIUS e TACACS+	Obrigatório
	5.3		Deve implementar filtros de ACL, permitindo a elaboração de regras.	Obrigatório
	5.4		Implementar grupos de usuários com diferentes níveis de acesso, ou possuir pelo menos 3 grupos de usuários pré-definidos. Deverá possuir um controle de comandos para usuários ou grupos no equipamento.	Obrigatório
	5.5		Implementar Private VLAN ou funcionalidade similar que permita segmentar uma VLAN em subdomínios: uma VLAN primária e múltiplas VLANs secundárias.	Obrigatório
	5.6		O equipamento deve incluir proteção contra-ataques de negação de serviço (denial of service).	Obrigatório
	5.7		O equipamento deve prover mecanismos de detecção e supressão de ataques do tipo ARP.	Obrigatório

Subitem		Característica	Especificação	Exigências
Qualidade de serviço	6.1	QoS	Implementar Qualidade de Serviço (QoS), de acordo com o padrão IEEE 802.1p (priorização de tráfego por porta).	Mínimo Obrigatório
	6.2		Deverá implementar no mínimo 7 (sete) filas de QoS por porta baseada em hardware.	Mínimo Obrigatório
	6.3		Implementar Qualidade de Serviço (QoS) de acordo com a RFC 2474, ou RFC 2475 (An Architecture for Differentiated Service), ou equivalente.	Mínimo Obrigatório
	6.4		Implementar os algoritmos de gerenciamento de filas: Deficit Weighted Round Robin (DWRR), ou Weighted Round Robin (WRR), ou Deficit Round Robin (DRR), ou Weighted Fair Queuing (WFQ) e Strict Priority (SP), ou Weighted Tail-Drop (WTD) como mecanismo de prevenção de congestionamento.	Mínimo Obrigatório
	6.5		Implementar classificação e marcação de pacotes baseada em CoS (Class of Service) padrão IEEE 802.1p.	Obrigatório
	6.6		Implementar classificação e marcação de pacotes baseada em marcação DSCP.	Obrigatório
	6.7		Implementar classificação e marcação de pacotes baseada em: endereço de origem, porta de origem, endereço de destino, porta de destino.	Obrigatório

Subitem		Característica	Especificação	Exigências
Demais Condições	7.1	Certificado	Possuir homologação da ANATEL, de acordo com a resolução número 242 de 30/11/2000.	Obrigatório
	7.2	Firmware	A versão da placa (ou módulo) de gerenciamento, ou de qualquer outro módulo existente no equipamento, e seus respectivos programas de controle (on-board ou não) deverão ser os mais atuais existentes no momento da entrega do equipamento.	Obrigatório
	7.3		Novas versões e/ou patches dos softwares integrantes da solução ofertada (on-board ou não) dos módulos do equipamento deverão ser fornecidas gratuitamente durante o período de garantia. Estas versões deverão ser fornecidas pelo fabricante num período máximo de 60 (sessenta) dias após sua divulgação no mercado, devendo a CONTRATADA prestar suporte técnico telefônico para o procedimento de atualização.	Obrigatório
	7.4		A cada atualização realizada deverão ser fornecidos os manuais técnicos originais e documentos comprobatórios do licenciamento da nova versão/patch.	Obrigatório
Características físicas	8.1		Deve possuir fonte de alimentação com capacidade de operar em tensões de 100 a 240 V e em frequências de 50/60 Hz.	Mínimo Obrigatório

Subitem		Característica	Especificação	Exigências
	8.2		O equipamento será destinado ao uso em ambiente com umidade relativa na faixa de 20 a 80% (sem condensação) e temperatura ambiente na faixa de 5 a 40 °C.	Mínimo Obrigatório
	8.3		O equipamento deverá vir acompanhado de cabos de força, acessórios e cabo de acesso a console do equipamento para configuração do mesmo.	Mínimo Obrigatório
	8.4		O equipamento deverá vir acompanhado de todos os módulos e/ou dispositivos necessários para seu perfeito funcionamento e operação, em conformidade com as especificações técnicas aqui apresentadas, mesmo que esses não constem desta especificação.	Mínimo Obrigatório
	8.5		O equipamento deverá possuir manual de todos os dispositivos e softwares que acompanham o conjunto. Toda documentação – manuais, guia de usuário, recomendações, etc., deverá ser fornecida em papel ou mídia magnética (formato PDF ou CHM), em língua portuguesa ou inglesa.	Obrigatório

4. Access Point

Compatibilidade: Do mesmo fabricante e compatível com a controladora de rede sem fio prevista neste anexo.

Subitem		Características	Especificações	Exigência
Características	1.1	Tipo	Wireless Access Point tecnologia 802.11a/b/g/n/ac com compatibilidade a ser gerenciado remotamente por controlador de rede wireless.	Obrigatório
	1.2	Padrões IEEE	802.11a, 802.11b, 802.11g, 802.11n, 802.11ac.	Mínimo Obrigatório
	1.3	Certificações Wi-Fi	WMM (Wi-Fi Multimedia) e Anatel.	Mínimo Obrigatório
	1.4	Monitor de radiofrequência	O equipamento deve suportar operação simultânea como Ponto de Acesso (*Access Point*) e monitor de Radiofrequência.	Obrigatório
	1.5	Modo gerenciado	Deve implementar funcionamento em modo gerenciado por controladora WLAN, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS, monitorização de RF (rádio freqüência). O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento nível 3 da camada OSI.	Obrigatório
	1.6	Ajuste dinâmico de potência	Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF conforme as características do ambiente.	Obrigatório

Subitem		Características	Especificações	Exigência
	1.7	Taxas de Transmissão	IEEE 802.11a/g: 54 Mbps.	Mínimo Obrigatório
	1.8		IEEE 802.11b: 11 Mbps	Mínimo Obrigatório
	1.9		IEEE 802.11n: 300 Mbps	Mínimo Obrigatório
	1.10		IEEE 802.11ac: 866 Mbps	Mínimo Obrigatório
	1.10	Firmware	Atualizável.	Obrigatório
	1.11	Liga/desliga	Controle para Ligar e Desligar o sinal wireless e SSID.	Mínimo Obrigatório
	1.12	SSID	Possuir suporte a pelo menos 16 SSIDs.	Obrigatório
	1.13	Interface de rede	Porta RJ-45 10/100/1000 Base-T, compatível com 802.3af porta Poe com auto negociação.	Mínimo Obrigatório
	1.14	Seleção de canal	Deve possuir capacidade de selecionar automaticamente o canal de transmissão.	Obrigatório
	1.15	Frequência de operação	2,4GHz e 5Ghz de forma simultânea (*dual-band).*	Obrigatório
	1.16	Indicadores	LED(s) indicador(es) de ligado e status.	Mínimo Obrigatório
	1.17	Montagem e trava de segurança	Deve permitir montagem em parede, incluindo suporte com local apropriado para cadeado ou trava antifurto, incluindo todos os acessórios e/ou parafusos necessários. Deverá também estar incluso o cadeado ou trava antifurto com chave.	Obrigatório
	1.18	Quantidade de usuários	Não deve haver licenciamento restringindo o número de usuários por ponto de acesso.	Obrigatório

Subitem		Características	Especificações	Exigência
	1.19	Usuários simultâneos	Capacidade para 100 (cem) usuários conectados simultaneamente em um equipamento.	Mínimo Obrigatório
	1.20	QoS	Suporte a alocação dinâmica de banda com priorização de aplicações (IEEE 802.11e).	Obrigatório
	1.21	Antenas	Deverá possuir 2 antenas com MIMO 2x2 (transmite em duas antenas e recebe em 2) e padrão de irradiação omnidirecional. Ganho no mínimo 2 dBi para 2,4 GHz. Ganho no mínimo 3 dBi para 5,0 GHz.	Mínimo Obrigatório
	1.22	Protocolos	CSMA/CA TCP/IP (IPv4 e IPv6)	Mínimo Obrigatório
	1.23	VLAN	Implementar a criação de pelo menos 16 VLANs.	Obrigatório
	1.24	Varredura de RF	Possibilitar a detecção de intrusão ao varrer múltiplas faixas e canais para localizar APs não autorizados e redes wireless *peer-to-peer*.	Obrigatório
	1.25	Bloqueio de intrusos	O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e bloqueio de intrusos no ambiente *wireless*.	Obrigatório
	1.26	Comunicações Ad-Hoc	Implementar, em conjunto com o Controlador WLAN, mecanismos para detecção na rede *wireless* de estações de trabalho que estejam realizando comunicações *ad-hoc*.	Obrigatório
	1.27	Balanceamento de carga	Deve suportar balanceamento de carga de modo automático.	Obrigatório

Subitem		Características	Especificações	Exigência
	1.27	Bloqueio de configuração	Permitir a configuração do Ponto de Acesso via rede wireless.	Obrigatório
	1.28	VLAN para visitante	Implementar VLAN para que usuários não autenticados ganhem acesso restrito na condição de visitante.	Obrigatório
	1.29	Associação de usuário a VLAN	Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação.	Obrigatório
	1.30	ACL	Implementar associação dinâmica de QoS por usuário, com base nos parâmetros da etapa de autenticação.	Obrigatório
	1.31	Criptografia	Implementar criptografia do tráfego local.	Obrigatório
	1.32	Cliente DHCP	Implementar cliente DHCP, para configuração automática de rede.	Obrigatório
	1.33	Configuração automática	Deve configurar-se automaticamente ao ser conectado na rede.	Obrigatório
	1.34	Protocolos de segurança de autenticação e criptografia	Criptografia WPA2 AES e TKIP; Criptografia 64/128; Autenticação 802.1x com EAP-TLS, EAP-TTLS, PEAP; WPAPSKa; Autenticação e filtro por MAC address; 802.1Q VLAN; Múltiplo SSID.	Mínimo Obrigatório
	1.35	Compatibilidade Normas de segurança	IEC ou UL 60950	Mínimo Obrigatório
	1.36	Gerenciamento	Acesso para gerência do dispositivo através de: Browser (http/HTTPS) SNMP V.1 e V.2	Mínimo Obrigatório

Subitem		Características	Especificações	Exigência
Alimentação	2.1	PoE	Compatível com PoE (Power Over Ethernet) IEEE 802.3af.	Obrigatório
Documentação	3.1	Manuais	O equipamento deverá possuir manual de todos os dispositivos e softwares que acompanham o conjunto. Toda documentação – manuais, guia de usuário, recomendações, etc., deverá ser fornecida em papel ou mídia magnética (formato PDF ou CHM), em língua portuguesa ou inglesa.	Obrigatório

5. Controladora rede sem fio

Compatibilidade: Capacidade para configurar e gerenciar o Access Point constantes neste anexo.

A controladora poderá ser física, virtual ou incorporada no Access Point.

Subitem		Características	Especificação	Exigência
Recursos	1.1	Tipo	Controlador Wireless LAN – com capacidade para configurar e gerenciar os Access Points compatíveis, a partir de um ponto central da rede.	Obrigatório
	1.2	Padrões IEEE	Compatível com 802.11a/b/g/n/ac.	Mínimo Obrigatório
	1.3	Número de portas	Se física, 4 (quatro) portas Gigabit Ethernet.	Mínimo Obrigatório
	1.4	Capacidade de gerenciamento de Access Points	Deverá ser ofertado com capacidade para gerenciamento de no mínimo 200 (duzentos)	Mínimo Obrigatório

Subitem		Características	Especificação	Exigência
			Access Points, com um número mínimo de 50 (cinquenta) licenças incluídas.	
	1.5	Firmware	Atualizável.	Obrigatório
	1.6	Configuração	Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.	Obrigatório
	1.7	Localização dos Pontos de Acesso	Os Pontos de Acesso gerenciados pelo Controlador WLAN poderão estar conectados localmente (LAN) ou, remotamente (WAN), inclusive via roteamento de nível 3 da camada OSI.	Obrigatório
	1.8	Syslog	Permitir a gravação de eventos por meio de *syslog*.	Obrigatório
	1.9	Mesh	Permitir operação em modo mesh.	Obrigatório
	1.10	Ajuste de parâmetros de RF	Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF.	Obrigatório
	1.11	Balanceamento de carga	Implementar sistema de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos, para otimizar a performance.	Obrigatório

Subitem		Características	Especificação	Exigência
	1.12	Ajuste do nível de potência	Ajustar dinamicamente o nível de potência e canal de rádio dos Pontos de Acesso, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade.	Obrigatório
	1.13	Roaming	Possibilitar *roaming* com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoWLAN e *streaming* de vídeo.	Obrigatório
	1.14	Servidor DHCP	Implementar servidor DHCP ou DHCP relay.	Obrigatório
	1.15	Cluster	Capacidade de funcionamento série ou paralelo de modo a prover redundância com prevenção a falhas.	Obrigatório
Qualidade de Serviço	2.1	QoS	WiFi Multimedia (WMM®)	Mínimo Obrigatório
	2.2		Suporte a Qos da rede via DiffServ Marking e 802.1p	
Administração	4.1	Interfaces de administração	Web-based: para os protocolos HTTP/HTTPS. Linha de Comando para Telnet ou SSH e porta do console.	Mínimo Obrigatório
	4.2	Software	Deverá ser fornecido o software para configuração centralizada tanto do equipamento quanto para o gerenciamento das *farms* de Access Points remotos.	Mínimo Obrigatório
	4.3	Demais padrões de administração	SNMP v1, v2 e v3 Permitir a gravação de eventos por meio de *syslog*.	Mínimo Obrigatório

Subitem		Características	Especificação	Exigência
Interfaces e Indicadores	5.1	Interfaces e indicadores	Se física, indicadores LED de atividade de link Portas: 10/100/1000 Mbps Ethernet (RJ45) Console Port Outros indicadores: Status, Power	Mínimo Obrigatório
	6.1	Tunelamento	Suportar estabelecimento de túneis seguros numa rede IP (na camada três, sem necessidade de alteração da infraestrutura básica da rede) entre o Controlador e os AP´s para tráfego dos dados entre esses dois equipamentos.	Obrigatório
	6.2	Localização de usuários	Suportar a implementação de sistema de localização de usuários.	Obrigatório
	6.4	Integração com RADIUS	Integração com Radius Server que suporte os métodos EAP citados no subitem 6.3.	Obrigatório
	6.5	Associação de usuário a VLAN	Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação.	Obrigatório
	6.6	Associação de ACL e QoS	Implementar associação dinâmica de QoS por usuário, com base nos parâmetros da etapa de autenticação	Obrigatório
	6.7	Limitação de Banda	Permitir a limitação de banda por usuário ou por WLAN.	Obrigatório

Subitem		Características	Especificação	Exigência
	6.8	Acesso a usuário *guest*	O sistema deverá permitir que seja configurado um perfil para o qual será direcionado o usuário que não consiga se autenticar (acesso *guest*).	Obrigatório
	6.9	Criptografia	WEP e TKIP-MIC: RC4 40, 104 bits SSL and TLS AES: CCM, CCMP	Mínimo Obrigatório
	6.10	Padrões de segurança	WPA IEEE 802.11i (WPA2, RSN) IEEE 802.1X IEEE 802.11d IEEE 802.11h RFC 2246 TLS Protocol Version 1.0	Mínimo Obrigatório
Sistema de Prevenção de	7.1	IPS	Possuir mecanismos de *WIPS (Wireless Intrusion Prevention System)*, no próprio Controlador ou em dispositivo externo específico para essa função.	Mínimo Obrigatório
Alimentação	8.1	Rede Elétrica	Se física, tensão de operação: 100-240 VAC, 5060 Hz	Mínimo Obrigatório
Fatores Ambientais	9.1	Fatores ambientais de operação e armazenamento	Se física, Temperatura de Operação: 0°C até 40°C Umidade Relativa do Ar de Operação e Armazenamento: 5% até 85% sem condensação.	Mínimo Obrigatório
Dispositivos	10.1	Cabos	Se física, o equipamento deverá vir acompanhado de cabos de força, acessórios e cabo de acesso a console do	Mínimo Obrigatório

Subitem		Características	Especificação	Exigência
			equipamento para sua configuração.	
	10.2	Módulos	O equipamento deverá vir acompanhado de todos os módulos e/ou dispositivos necessários para seu perfeito funcionamento e operação, em conformidade com as especificações técnicas aqui apresentadas, mesmo que esses não constem desta especificação.	Mínimo Obrigatório
Documentação	11.1	Manuais	O equipamento deverá possuir manual de todos os dispositivos e softwares que acompanham o conjunto. Toda documentação – manuais, guia de usuário, recomendações etc., deverá ser fornecida em papel ou mídia magnética (formato PDF ou CHM), em língua portuguesa ou inglesa.	Obrigatório

6. NAC

Grupo	Item	Descrição	Especificação Mínima
Características Gerais	CG1	Solução para controlar o acesso de usuários à rede.	Obrigatório
	CG2	Deverá ser fornecido em equipamento autônomo, ou seja, módulo (hardware) projetado especificamente para atender a solução, acompanhado do sistema operacional (software) otimizado para esse fim.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	CG3	A solução deverá ser totalmente integrada e compatível com todos os equipamentos de rede e segurança oferecidos.	Obrigatório
	CG4	Deve vir com todo hardware, software e licenças necessárias para suportar no mínimo 500 usuários simultâneos em um appliance ou em um conjunto de appliances e/ou applience virtual.	Obrigatório
	CG5	Deverá vir acompanhado do software de gerenciamento centralizado da solução na quantidade / modelo necessário para atender a solução completa desta solicitação;	Obrigatório
	CG6	Reconhecer e autenticar o usuário através de políticas definidas por regras permitindo, isolando ou bloqueando o usuário/dispositivo a acessar os recursos da rede;	Obrigatório
	CG7	A estação de trabalho do usuário pode ter acesso via LAN, WLAN ou VPN, esta última com no mínimo 500 usuários;	Obrigatório
Autenticação	AT1	Deve implementar a autenticação com servidor Radius externo para a autenticação de usuários da rede, com suporte a autenticação IEEE 802.1x. Caso o fornecedor utilize o sistema de autenticação em conjunto com switch, esta funcionalidade deverá estar presente no switch de acesso.	Obrigatório
	AT2	Deve implementar a autenticação com servidor Radius externo para a autenticação de usuários da rede via o MAC Address de origem; Caso o fornecedor utilize o sistema de autenticação em conjunto com switch, esta funcionalidade deverá estar presente no switch de acesso.	Obrigatório
	AT3	Registrar a localização e informação do usuário autenticado na rede de forma automática, incluindo ao menos 2 dos seguintes itens: - switch e a porta do switch onde o usuário está conectado	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
		- endereço MAC - endereço IP do usuário - Username (caso seja autenticação 802.1x) - resultado da autenticação e a ação tomada pela solução;	
	AT4	Programa cliente para ser executado sobre o sistema operacional Windows XP, Windows Vista ou MacOS; ou ainda pode independer do agente (programa cliente) e ser redirecionado para um portal de autenticação.	Obrigatório
Auditoria	AU1	Suportar a verificação de postura de sistemas remotos com sistema operacional: Windows (XP, 2003, Vista), MacOS, e Linux	Obrigatório
	AU2	Suportar verificação com agente temporário (agent-based) e sem agente (network-based)	Obrigatório
	AU3	Realizar pré-checagem de conformidade da atualização dos programas na estação de trabalho do usuário, incluindo verificação de segurança End Point, atualização e correção para sistema operacional (automático ou através de aceite do usuário), evitando assim que a estação introduza código malicioso no sistema da rede.	Obrigatório
	AU4	As políticas e regras de acesso devem variar com análise de não conformidade da estação de trabalho do usuário, podendo remeter o usuário para uma sub-rede para reparação ou atualização dos programas.	Obrigatório
Autorização	AR1	Permitir criar múltiplos perfis de usuários, baseado em regras de controle de acesso, a ser aplicada no controle de acesso à rede, criando diferentes níveis de privilégios de uso.	Obrigatório
	AR2	Dispositivo capaz de admitir integração com MS-AD para um único login do usuário (single sign on = SSO).(Podendo utilizar Radius)	Obrigatório
	AR3	Permitir fazer a revalidação de acesso à rede periodicamente; em intervalos pré-definidos;	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	AR4	Permitir o controle de acesso à rede nas camadas do modelo OSI 2 ou 3; Caso o fornecedor utilize o sistema de autenticação em conjunto com switch, esta funcionalidade deverá estar presente no mesmo.	Obrigatório
	AR5	Permitir funcionar em alta-disponibilidade, dispositivo primário e secundário, trabalhando de forma redundante. Em caso de falha do primeiro, o segundo entra em operação de forma transparente para o usuário.	Obrigatório
	AR6	Deve permitir a criação de perfis de usuários com requisitos de segurança diferentes para cada perfil	Obrigatório
	AR7	Deve suportar aplicação das regras diretamente nos switches de acesso, através de controle de regras de segurança ou VLANs, com suporte ao padrão RFC 3580 (VLAN Authorization).	Obrigatório
	AR8	Deve suportar uma pagina HTML de convidados para registro de endereços MAC onde:	Obrigatório
	AR9	Deve permitir a configuração de listas de exceções por nome de usuário, endereço MAC, ou grupos de endereço MAC ou utilizando MAB (MAC Authentication Bypass)	Obrigatório
	AR10	Para cada perfil de usuário a solução deverá implementar a validação da máquina do usuário antes do acesso a rede. Essa validação deverá verificar no mínimo: • Versão do Sistema Operacional Instalado • Verificação do Service Pack Instalado • Pesquisa de Chaves de Registro • Existência de Software de segurança End Point Instalado • Status do software Antivírus (Habilitado ou Desabilitado ou Atualizado ou Não Atualizado) • Processo em memória	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	AR11	Deverá permitir a verificação da versão da última assinatura de antivírus fornecida pelos principais players de antivírus.	Obrigatório
	AR12	Deverá permitir a verificação dos Hotfixes disponibilizados pela Microsoft para cada um dos sistemas operacionais suportados.	Obrigatório
	AR13	Cada usuário (interno ou externo) deverá ser associado a um perfil de usuário.	Obrigatório
	AR14	Para cada perfil de usuário deverá ser possível a criação de pré-requisitos para que a estação tenha acesso total à rede. Esses pré-requisitos devem ser baseados na verificação dos itens mencionados anteriormente nessa especificação (sistema operacional, antivírus, hotfix, processo, etc)	Obrigatório
	AR15	Caso a estação não esteja de acordo com os requisitos necessários para o perfil do usuário, a solução deverá isolar a estação e informar ao usuário que a máquina não está de acordo com as políticas de segurança.	Obrigatório
	AR16	Caso o usuário possua o cliente instalado (agente) esse agente deverá guiar o usuário no processo de atualização da estação (provendo links para os patches, atualização do software de antivírus, etc) a fim de que a estação fique de acordo com as políticas de segurança.	Obrigatório
	AR17	A solução não deverá permitir que o cliente instalado (agente) tome nenhuma ação na máquina do usuário (instalação de programas automaticamente).	Obrigatório
Gerenciamento	GR1	Gerenciamento para configuração e alterações das regras e políticas através de interface gráfica WEB;	Obrigatório
	GR2	Deve permitir verificar e monitorar o estado operacional do servidor;	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	GR3	Realizar a comunicação entre o servidor e o gerenciamento através de modo seguro utilizando SSL (Secure Socket Layer) ou outro modo com criptografia; caso haja falha de comunicação entre ambos, deve poder configurar a política para usuário entre permitir, ignorar ou bloquear o trafego do usuário.	Obrigatório
	GR4	Deve permitir a autenticação (via Radius) dos usuários nas bases de dados: • LDAP • Windows Active Directory	Obrigatório
	GR5	Deverá permitir a criação de usuários na base local	Obrigatório
	GR6	A solução deve ser fornecida em dispositivos de hardware dedicados para essa função (appliance).	Obrigatório
	GR7	Todos os dispositivos de hardware deverão implementar redundância do tipo ativo-standby. Na falha de qualquer dispositivo ativo o dispositivo redundante deverá assumir todas as funções. Deverão ser fornecidos ambos dispositivos (Ativo e Standby)	Obrigatório
	GR8	A solução de acesso físico à rede deverá ser totalmente compatível com os equipamentos de switch deste edital evitando problemas de interoperabilidade.	Obrigatório

7. Firewall

Grupo	Item	Descrição	Especificação Mínima
Solução Integrada	SI1	Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, malwares, Filtro de URL e Sandbox para análise de malwares desconhecidos. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.	Obrigatório
	SI2	Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / malwares, endpoints, assinaturas de IPS, filtro de conteúdo web, controle de aplicações sem custo adicional, pelo período mínimo de 36 (trinta e seis) meses.	Obrigatório
	SI3	Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.	Obrigatório
	SI4	Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.	Obrigatório
	SI5	A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um equipamento para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	SI6	Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.	Obrigatório
	SI7	A solução deverá possuir interface de administração via web.	Obrigatório
Capacidade e Desempenho	CD1	Performance mínima de throughput para firewall.	20 Gbps
	CD2	Performance mínima de *throughput* de IPS.	2.2 Gbps
	CD3	Performance mínima de throughput para controle de AV/proxy.	2.8 Gbps
	CD4	Performance mínima de *throughput* de VPN.	1.7 Gbps
	CD5	Suporte a, no mínimo de conexões simultâneas.	8.200.000
	CD6	Suporte a, no mínimo, novas conexões por segundo.	200.000
	CD7	Possuir o número irrestrito quanto ao máximo de usuários licenciados.	Obrigatório
	CD8	Possuir visor LCD para verificação de configurações.	Obrigatório
	CD9	Possuir armazenamento interno para quarentena local, logs e relatórios.	Obrigatório
Imterfaces	IT1	Possuir no mínimo 8 (Oito) interfaces de rede 1000Base-TX.	8 (oito)
	IT2	Possuir no mínimo 2 (duas) interfaces que atuem em modo de by-pass.	2 (duas)
	IT3	Possuir no mínimo 2 (duas) interfaces SFP.	2 (duas)
	IT4	Possuir no mínimo 2 (duas) interfaces 10GbE SFP+.	2 (duas)
	IT5	Permitir instalação de no mínimo 1 (um) módulo de expansão de interfaces.	1 (um)
	IT6	Possuir 1 (uma) interface do tipo console ou similar.	1 (uma)

Grupo	Item	Descrição	Especificação Mínima
	IT7	Possuir 2 (duas) fontes redundantes100-240VAC interna ou externa.	2 (duas)
Características Gerais	CG1	A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs.	Obrigatório
	CG2	Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.	Obrigatório
	CG3	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.	Obrigatório
	CG4	O software deverá ser fornecido em sua versão mais atualizada.	Obrigatório
	CG5	Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.	Obrigatório
	CG6	A atualização de software deverá enviar avisos de atualização automáticos.	Obrigatório
	CG7	O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.	Obrigatório
	CG8	O backup e o reestabelecimento de configuração deverão ser feito localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.	Obrigatório
	CG9	Deve ser possível criar backup das configurações protegido por senha.	Obrigatório
	CG10	As notificações deverão ser realizadas via email e SNMP.	Obrigatório
	CG11	Suportar SNMP e Netflow.	Obrigatório
	CG12	O firewall deverá ser stateful, com inspeção profunda de pacotes (deep packet inspection).	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	CG13	As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.	Obrigatório
	CG14	As políticas de NAT deverão ser customizáveis para cada regra.	Obrigatório
	CG15	A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS) e bloqueio de portscan.	Obrigatório
	CG16	Proteção contra anti-spoofing.	Obrigatório
	CG17	Suportar IPv4 e IPv6.	Obrigatório
	CG18	IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.	Obrigatório
	CG19	Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).	Obrigatório
	CG20	Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.	Obrigatório
	CG21	O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.	Obrigatório
	CG22	A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;	Obrigatório
	CG23	A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;	Obrigatório
	CG24	O traffic shapping (QoS) deverá ser baseado em rede ou usuário.	Obrigatório
	CG25	A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.	Obrigatório
	CG26	Deve possuir otimização em tempo real de voz sobre IP.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	CG27	Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).	Obrigatório
Controle por Políticas de Firewall	CFW1	Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.	Obrigatório
	CFW2	O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.	Obrigatório
	CFW3	As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.	Obrigatório
	CFW4	Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.	Obrigatório
	CFW5	Controle de políticas por países via localização por IP.	Obrigatório
	CFW6	Suporte a objetos e regras IPV6.	Obrigatório
	CFW7	Suporte a objetos e regras multicast.	Obrigatório
Prevenção de Ameaças	PA1	Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, Anti-Malware e Firewall de Proteção Web (WAF) integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.	Obrigatório
	PA2	Deve realizar a inspeção profunda de pacotes (DPI deep packet inspection) para prevensão de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).	Obrigatório
	PA3	Deve realizar a inspeção profunda de pacotes (DPI deep packet inspection) para prevensão de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	PA4	Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;	Obrigatório
	PA5	Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;	300
	PA6	A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP ;	Obrigatório
	PA7	A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.	Obrigatório
	PA8	Deve ter proteção em tempo real contra novas ameaças criadas.	Obrigatório
	PA9	Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.	Obrigatório
	PA10	Deve permitir o bloqueio de vulnerabilidades.	Obrigatório
	PA11	Deve permitir o bloqueio de exploits conhecidos.	Obrigatório
	PA12	Deve detectar e bloquear o tráfego de rede que busque acesso a contact command e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.	Obrigatório
	PA13	Deve incluir proteção contra-ataques de negação de serviços.	Obrigatório
	PA14	Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc.	Obrigatório
	PA15	Suportar bloqueio de arquivos por tipo.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	PA16	Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.	Obrigatório
	PA17	Os eventos devem identificar o país de onde partiu a ameaça.	Obrigatório
	PA18	Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.	Obrigatório
	PA19	Deve possuir pelo menos duas engines de anti-vírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.	Obrigatório
	PA20	Proteção pelo menos contra os seguintes ataques, mas não limitado a: SQL injection e Cross-site scripting.	Obrigatório
	PA21	Possui solução de sandbox para realizar análise de malwares desconhecidos em ambiente controlado na nuvem.	Obrigatório
	PA22	A solução de sandbox deve ser integrada a console de gerenciamento do firewall.	Obrigatório
	PA23	Deve realizar análise de arquivos executáveis do Windows, .exe, .com e .dll.	Obrigatório
	PA24	Deve realizar análise de arquivos MS Word em busca de malwares, como .doc, .docx e .rtf.	Obrigatório
	PA25	Deve realizar análise de arquivos do tipo PDF.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	PA26	Deve realizar análise de arquivos compactados, como ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z e Microsoft Cabinet.	Obrigatório
	PA27	A solução de sandbox deverá ter um tempo médio de análise inferior a 120 (cento e vinte) segundos.	Obrigatório
Controle e Proteção de Aplicações	CP1	Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.	Obrigatório
	CP2	Reconhecer pelo menos 3.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.	Obrigatório
	CP3	Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
		Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.	
	CP4	Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)	Obrigatório
	CP5	O escaneamento de micro app deverá ser habilitado via console gráfica (GUI) e via comando de linha (CLI).	Obrigatório
	CP6	Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.	Obrigatório
	CP7	Atualizar a base de assinaturas de aplicações automaticamente.	Obrigatório
	CP8	Reconhecer aplicações em IPv6.	Obrigatório
	CP9	Limitar a banda usada por aplicações (traffic shaping).	Obrigatório
	CP10	Deve possuir a funcionalidade de CASB (Cloud Access Security Broker) para identificar o tráfego das aplicações em nuvem.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	CP11	Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.	Obrigatório
	CP12	Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.	Obrigatório
	CP13	Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuirem acesso a estes aplicativos devem ter a utilização bloqueada.	Obrigatório
Controle e Proteção Web	CW1	Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.	Obrigatório
	CW2	Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.	Obrigatório
	CW3	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Radius, E-directory e base de dados local.	Obrigatório
	CW4	Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	CW5	Possuir pelo menos 90 categorias de URLs.	Obrigatório
	CW6	Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.	Obrigatório
	CW7	Deve ser capaz de forçar o uso da opção Safe Search em sites de busca.	Obrigatório
	CW8	Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário.	Obrigatório
	CW9	Suportar a criação categorias de URLs customizadas.	Obrigatório
	CW10	Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.	Obrigatório
	CW11	Permitir a customização de página de bloqueio.	Obrigatório
	CW12	Suportar a inclusão nos logs do produto de informações das atividades dos usuários.	Obrigatório
	CW13	Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado. Deve realizar caching do conteúdo web.	Obrigatório
	CW14	Deve relizar filtragem por mime-type, extensão e tipos de conteúdos ativos, tais como, mas não limitado a: ActiveX, applets e cookies.	Obrigatório
Identificação de Usuários	ID1	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	ID2	Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).	Obrigatório
	ID3	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.	Obrigatório
	ID4	Deve permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.	Obrigatório
	ID5	Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.	Obrigatório
	ID6	Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.	Obrigatório
Qualidade de Serviço - Qos	QS1	Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	QS2	A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.	Obrigatório
	QS3	Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado.	Obrigatório
	QS4	Suportar priorização Real-Time de protocolos de voz (VoIP).	Obrigatório
Redes Virtuais Privadas - VPN	VPN1	Suportar VPN Site-to-Site e Cliente-to-Site.	Obrigatório
	VPN2	Suportar IPsec VPN.	Obrigatório
	VPN3	Suportar SSL VPN.	Obrigatório
	VPN4	Suportar L2TP e PPTP.	Obrigatório
	VPN5	Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.	Obrigatório
	VPN6	Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL para estações Windows.	Obrigatório
	VPN7	Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.	Obrigatório
	VPN8	Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, HTTP, HTTPS, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	VPN9	A VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).	Obrigatório
	VPN10	Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.	Obrigatório
	VPN11	Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.	Obrigatório
	VPN12	Suportar autenticação via AD/LDAP, Token e base de usuários local.	Obrigatório
	VPN13	Permitir estabelecer um túnel SSL VPN com uma solução de autienticação via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local.	Obrigatório
Condições Operacionais	CD1	Alimentação (tensão).	220 VAC
	CD2	Alimentação / frequência.	60 Hz

8. Gerência

Grupo	Item	Descrição	Especificação Mínima
Características Gerais	CG1	Solução proposta: Configurada com licença para gerenciamento de número ilimitado de dispositivos ou todas licenças necessárias para atendimento a demanda	Obrigatório
	CG2	Deve prover interface de gerenciamento através dos protocolos HTTP e HTTPS compatível com os browsers padrões de mercado, como Microsoft IE versão 6 ou superior e Mozilla Firefox versão 3 ou superior	Obrigatório
	CG3	Deve permitir a configuração e o gerenciamento de Vlans de forma centralizada.	Obrigatório
	CG4	Deve permitir a configuração e o gerenciamento de ACLs de forma centralizada.	Obrigatório
	CG5	Deve possibilitar o gerenciamento através de SNMP v3, 4 grupos de RMON (caso o equipamento gerenciado suporte os 4 grupos) e scripts de configuração.	Obrigatório
	CG6	Deve permitir atualização de firmware dos produtos ofertados.	Obrigatório
	CG7	Deve permitir realizar backups/restore das configurações dos elementos de rede.	Obrigatório
	CG8	Deve receber as notificações via traps SNMP e mensagens Syslog permitindo buscas por dispositivo de origem e severidade da mensagem.	Obrigatório
	CG9	Deve possibilitar a notificação de eventos através de e-mail.	Obrigatório
	CG10	Deve permitir a geração de relatórios gráficos ou visualização na tela de gerência de estatísticas de utilização por portas, por MAC addresses, por IP, por aplicação, ou por usuários 802.1x	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
	CG11	Deve exibir os mapas da rede de forma gráfica permitindo a visualização da rede por topologias de IP e de Vlans	Obrigatório
	CG12	Deve possuir a facilidade de "auto discovery" de elementos de rede.	Obrigatório
	CG13	Deve suportar perfis de usuários com níveis de privilégio diferentes suportando ao menos usuários para somente leitura, leitura e escrita.	Obrigatório
	CG14	Deve suportar regiões administrativas permitindo o acesso ao gerente a um número restrito de equipamentos.	Obrigatório
	CG15	Deve permitir o gerenciamento de todos os agentes SNMP dos dispositivos que compõe a infra-estrutura de TI;	Obrigatório
	CG16	Deve permitir o descobrimento de equipamentos presentes em uma ou mais sub-redes, a fim de garantir uma auditoria constante na infraestrutura de TI; Deve permitir a criação de topologias / mapas automáticos da rede através de protocolos Layer 2 - O mapa deve permitir a identificação de problemas com os dispositivos visualmente; - Permitir a visão agrupada da topologia conforme configuração do usuário;	Obrigatório
	CG17	Deve permitir o gerenciamento das configurações de filas e priorização de tráfego dos dispositivos da rede;	Obrigatório
	CG18	Deve permitir a criação e o gerenciamento de políticas de acesso a rede nos dispositivos;	Obrigatório
	CG19	O software deve permitir a criação, edição, remoção de VLANs nos dispositivo e associação das portas as mesmas	Obrigatório
	CG20	A ferramenta deve permitir o inventário detalhado de atributos dos dispositivos da rede,	Obrigatório

Grupo	Item	Descrição	Especificação Mínima
		atendendo no mínimo números seriais, versão de firmware, tipo de CPU e memória;	
	CG21	A ferramenta deve permitir o armazenamento histórico das configurações dos dispositivos e permitir a comparação da configuração atual com a configuração armazenada;	Obrigatório
	CG22	A ferramenta deve possuir a capacidade de gerar relatórios de para planejamento de capacidade, atendendo no mínimo a geração de relatórios da utilização mínima de chassis e portas;	Obrigatório
	CG23	Deve permitir o upgrade da PROM de BOOT dos dispositivos, unitariamente e para um grupo de dispositivos;	Obrigatório

ANEXO IV – DECLARAÇÃO DE GARANTIA DE ASSISTÊNCIA TÉCNICA

A empresa _____,
com inscrição no CNPJ nº. _____, sediada na _____,
declara, sob as penas da lei, que durante todo o período de vigência do contrato, a assistência técnica, a manutenção corretiva e evolutiva de todos os equipamentos e softwares, bem como os que vierem a ser incorporados à infraestrutura da rede FAPEMIG, serão de sua inteira responsabilidade, devendo arcar com todos os seus custos, inclusive os decorrentes de intervenções por parte dos fabricantes dos equipamentos. Para os equipamentos da rede atual, a empresa garantirá a assistência técnica, manutenção corretiva e evolutiva, desde o início da vigência do contrato, para aqueles equipamentos que forem mantidos na infraestrutura de rede da FAPEMIG, observando os prazos de ativação das soluções estabelecidos no item 1.2.3.1.

Data e local

_____

Nome e assinatura do Diretor ou Representante Legal

ANEXO V – MODELO DE PROPOSTA COMERCIAL

À Fundação de Amparo à Pesquisa do Estado de Minas de Minas Gerais

[NOME DA EMPRESA PROPONENTE], sociedade com sede [ENDEREÇO], inscrita no CNPJ sob o nº . . / - , por meio de seu representante legal, firma a presente Proposta de Preços, que é baseada nas condições e prazos estabelecidos no Pregão Eletrônico planejamento nº XXXXXXXXXX/XXXX, os quais são aceitos pelo proponente, que se compromete a cumprir integralmente o objeto do Edital correspondente e do Contrato a ser firmado, de modo a entregar todos os produtos e serviços neles previstos.

PROPOSTA COMERCIAL PARA O PREGÃO ELETRÔNICO PROCESSO XX/2019
(preenchida em papel timbrado da proponente)
DADOS A CONSTAR NA PROPOSTA. PREENCHIMENTO PELA PROPONENTE.
Razão Social
CNPJ
Inscrição Estadual (se for o caso)
Inscrição Municipal
Endereço
Telefone/Fax
E-mail
Nome do(s) representante(s) legal(is) da empresa
Estado civil do representante legal
Nacionalidade do representante legal
Identidade do representante legal
CPF do representante legal
Preço Global da Proposta sem ICMS (R$): Preço Global da Proposta com ICMS (R$): Preço Global da Proposta sem ICMS (por extenso): Preço Global da Proposta com ICMS (por extenso):

Prazo de validade da proposta: 60 (sessenta) dias. Validade do Contrato: 36 (trinta e seis) meses, contados da data da publicação do contrato.
Pagamento conforme Edital. Indicar o nome do Banco – Agência e número de conta corrente do proponente onde deverá ser efetuado o pagamento.
Indicar o nome do Gerente de Projeto habilitado nesta licitação.
Data e local.
Assinatura do Representante Legal da Empresa

Lote – MANUTENÇÃO, OPERAÇÃO E GERENCIAMENTO DA REDE FAPEMIG

Infraestrutura	**Item**	**Descrição**	**Tipo**	**A=Qtde de IC***	**B=Valor Unitário Mensal (R$)**	**C=Valor Total Mensal (R$) = A x B**
	2	Enterasys SK1208-0808-F6	Módulo Fibra Ótica Switch Enterasys S8	1		
	3	Enterasys B5K125-48P2	Switch de distribuição	13		
	4	Enterasys B5G124-48P2	Switch de acesso	25		
	5	Enterasys B5G124-24P2	Switch de acesso	6		
	6	Enterasys WS-C5110-2-SR	Controladoras Wireless	1		
	7	Enterasys WS-AP3710I	Access Point	44		
	8	Enterasys NMS-BASE-50	Software de Gerenciamento	1		
	9	Enterasys NAC-A-20	Software de Gerenciamento	1		

Infraestrutura	Item	Descrição	Tipo	A=Qtde de IC*	B=Valor Unitário Mensal (R$)	C=Valor Total Mensal (R$) = A x B
Nova Solução	10					
	11					
	12					
	13					
	14					
	15					
-	-	D=Valor Total Mensal = (Σ C)				
-	-	E=Valor Total da Proposta = (D x 36 meses)				

*IC = Item de Configuração (Para a Infraestrutura atual, conforme relação dos itens 4.2 e 4.3 do ANEXO I - TERMO DE REFERÊNCIA)

OBSERVAÇÕES: Declarar expressamente que:

1) Os preços contidos nesta proposta incluem todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, taxa de administração, lucro, e outros custos necessários ao cumprimento integral do objeto deste Edital e seus Anexos, Quaisquer tributos, custos e despesas, diretos ou indiretos, omitidos da proposta ou incorretamente cotados, serão considerados como inclusos nos preços, não sendo considerados pleitos de acréscimos, a esse ou qualquer título, devendo os serviços ser fornecidos sem ônus adicionais.

2) Será levada em conta a Resolução Conjunta nº. 3458, de 22 julho de 2.003, das Secretarias de Estado da Fazenda e de Planejamento e Gestão, que regulamenta a isenção do ICMS para o caso de fornecedores situados no Estado.

PRAZO DE VALIDADE DESTA PROPOSTA:
DATA:
ASSINATURA DO REPRESENTANTE LEGAL:
CARIMBO: