**ANEXO I**

**TERMO DE REFERÊNCIA**

1. **OBJETO**

Contratação de empresa prestadora de serviços de locação de equipamentos de infraestrutura de rede corporativa, incluindo instalação, configuração e validação do funcionamento dos equipamentos, infraestrutura em nuvem (IAAS), suporte e manutenção especializada em informática, com a finalidade de acompanhamento, fornecimento de licenças, suporte necessário, bem como a aquisição de materiais de informática em geral para a Câmara Municipal, no município de Itaúna, sob o aspecto de segurança e confiabilidade dos dados processados, incluindo o acompanhamento mensal das rotinas de TI, visando consolidar os conceitos e a funcionalidade dos sistemas implantados, conferência dos backups, chamados de TI e acompanhamento geral dos ativos de rede da Câmara Municipal de Itaúna.

1. **DA JUSTIFICATIVA**

2.1. Considerando o e-mail recebido no dia 12/05/2022 enviado pela empresa Digital Informática, a qual tem contrato vigente na prestação de serviço com esta Casa de Leis, alertando em duas oportunidades (março e outubro de 2021) acerca da atual estrutura e segurança na área de TI, elencando atráves de diversos pontos a necessidade de melhorias e aperfeiçoamentos no tange toda a estrutura de infomática e tecnologia da Câmara Muncipal de Itaúna;

2.2. Considerando o e-mail datado do dia 16/05/2022, enviado pela Gerência Administrtiva e Financeira, no qual é proposto uma reunião a fim de definir quais as aquisições e serviços necessários para sanar os apontamentos apresentados no e-mail do dia 12/05/2022;

2.3. Considerando que a empresa que presta serviço na área de TI emprestou alguns switches evitando à época a paralização de algumas tarefas mais simples;

2.4. Considerando a necessidade de aquisição de novas licenças de softwares;

2.5. Considerando que no ano de 2021 foram adquiridos alguns produtos de informártica conforme Processo licitatório nº 46/2021 e, que ainda faltam outros equipamentos;

2.6. Por fim, com intuito de otimizar a qualidade da infraestrutura de rede, a qual irá proporcionar o acesso mais rápido, eficaz e seguro, permitindo a implantação do GED (Gerenciamento Eletrônico de Documentos), bem como melhorando de forma substancial a segurança dos dados e informações, é que se faz necessária tal contratação.

1. **DA DESCRIÇÃO E ESPECIFICAÇÃO**

**LOTE 01 (SERVIÇOS / LOCAÇÃO)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Item | Especificação | Unid. | Qtd. | Marca/ Modelo | Valor Unit. Mês | Valor 12 meses |
| 1 | Computação em nuvem para até 20 Máquinas Virtuais  **Especificação** detalhada consultar item 3.7 deste TR | Unid. | 01 |  |  |  |
| 2 | Backup Empresarial como Serviço para até 20 instancias com repositório na nuvem de até 20 TB **Especificação** detalhada consultar item 3.12 deste TR | Unid. | 01 |  |  |  |
| 3 | Antivírus corporativo para endpoints **Especificação** detalhada consultar item 3.13 deste TR | Unid. | 50 |  |  |  |
| 4 | Access Point Corporativo com Controladora centralizada. **Especificação** detalhada consultar item 3.14 deste TR | Unid. | 09 |  |  |  |
| 5 | Appliance de firewall NGFW com nobreak **Especificação** detalhada consultar item 3.15 deste TR | Unid. | 01 |  |  |  |
| 6 | Contrato de Prestação de Serviços **Especificação** detalhada consultar item 3.26 deste TR | Unid. | 01 |  |  |  |
| Valor Total do Lote 01 | | | | |  |  |

**LOTE 02 (AQUISIÇÃO)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Item | Especificação | Unid. | Qtd. | Marca/ Modelo | Valor Unit. |  |
| 1 | Switch 48 portas  **Especificação** detalhada consultar item 3.27 deste TR | Unid. | 05 |  |  |  |
| 2 | Licença Office Home and Business **Especificação** detalhada consultar item 3.28 deste TR | Unid. | 05 |  |  |  |
| 3 | Nobreaks 1500 VA **Especificação** detalhada consultar item 3.29 deste TR | Unid. | 05 | SMS  SUPERIOR OU EQUIVALENTE |  |  |
| 4 | Baterias para Nobreak 12V 18A, específica para nobreak  Referência: SMS Power Sinus II 3000VA | Unid. | 02 | Referência: SMS Power Sinus II 3000VA |  |  |
| 5 | Baterias para Nobreak 12V 17A, específica para nobreak  Referência: SMS Power Sinus 2400VA | Unid. | 02 | Referência: SMS Power Sinus 2400VA |  |  |
| 6 | Baterias para Nobreak 12V 07A, específica para nobreak  Referência: SMs Net Manager Net4+ 1400va | Unid. | 04 | Referência: SMs Net Manager Net4+ 1400va |  |  |
| 7 | Baterias para Nobreak 12V 05A, específica para nobreak  Referência: SMS Station II 1200va | Unid. | 02 | Referência: SMS Station II 1200va |  |  |
| 8 | **Memória DDR3 DESCRIÇÃO DO ITEM:**  Capacidade: 8 GB  Frequência: 1333 MHz  Tecnologia: DDR3  Formato: DIMM | Unid | 14 | KINGSTON SUPERIOR OU EQUIVALENTE |  |  |
| 9 | **SSD DESCRIÇÃO DO ITEM:**  Tecnologia de armazenamento: SSD  Capacidade mínina de : 240 GB  Velocidade de leitura: 500 MB/seg  Velocidade de escrita: 450 MB/seg  Interface: SATA III | Unid | 12 | KINGSTON SUPERIOR OU EQUIVALENTE |  |  |
| 10 | Fonte ATX 450 w nominal **DESCRIÇÃO DO ITEM:**  fonte atx 450w nominal/ conectores sata 2 /ide 2/ 12 v / 24 pinos | Unid | 06 | c3tech  SUPERIOR OU EQUIVALENTE |  |  |
| 11 | Estabelizador 300 VA Mono – preto. DESCRIÇÃO DO ITEM: Potência:300V Frequência:60Hz Voltagem: 115V (entrada e saída) Cor:Preto Material:Plástico Tomadas: 4 tomadas no padrão NBR14136 Botão Liga/Desliga: Temporizado | Unid | 20 | SMS  SUPERIOR OU EQUIVALENTE |  |  |
| 12 | Aparelho Telefone Com Fio   DESCRIÇÃO DO ITEM: campainha em 3 volumes (alto, médio e baixo) com 2 timbres, teclado com 15 teclas sendo 12 teclas numéricas e 3 teclas de funções (Redial, Flash, Mute) | Unid | 40 | Intelbras  SUPERIOR OU EQUIVALENTE |  |  |
| 13 | Adaptador VGA FÊMEA X HDMI MACHO | Unid | 04 |  |  |  |
| Valor Total Lote 02 | | | | |  |  |

* 1. A licitante deverá citar em sua proposta a marca e modelo dos materiais, sob pena de desclassificação.
  2. Todos os materiais ofertados deverão estar de acordo com as exigências constantes no Termo de Referência.
  3. CONTRATADA deverá fornecer a garantia dos itens constantes no Termo de Referência por período mínimo de 12 meses.
  4. Os materiais ofertados deverão atender às normas da Associação Brasileira de Normas Técnicas (ABNT) nos termos da Lei 4.150 de 21 de novembro de 1962, ainda que estas não estejam especificadas neste Edital.
  5. Os produtos NÃO NORMATIZADOS PELA ABNT deverão ser fornecidos de acordo com a disponibilidade de mercado, observados os requisitos mínimos de qualidade.
  6. DETALHAMENTOS DOS ITENS:
     1. Fornecimento dos hardwares:
     2. Os equipamentos deverão ser entregues no local indicado neste Termo de Referência, acondicionados adequadamente.
     3. Os equipamentos deverão ser fornecidos em caráter de locação pelo período de 12 meses.
     4. Os equipamentos deverão ser fornecidos com todos os itens, acessórios de hardware e software necessários à sua perfeita instalação e funcionamento mesmo que não descritos nas especificações acima, incluindo cabos, conectores, interfaces, suportes, drivers de controle, programas de configuração, dentre outros.
     5. Somente serão aceitas ofertas de componentes de especificação diferente da solicitada, no caso de igual ou superior qualidade, desempenho e operacionalidade, e que mantenham compatibilidade com os demais componentes da solução, conforme descrito neste Termo de Referência.
     6. A aceitação dos equipamentos no ato da sua entrega a Câmara Municipal de Itaúna será considerada como de caráter provisório. A aceitação definitiva dar-se-á após a fase de implantação, instalação e configuração dos referidos equipamentos e a verificação do atendimento às especificações técnicas constantes deste Termo de Referência.
     7. O prazo para a entrega dos equipamentos, em caráter provisório, será de até 60 (sessenta) dias corridos, contados a partir da data de emissão da Autorização de Empenho (AE).
     8. Especificações dos Itens de Hardware:
  7. Computação em Nuvem (Lote 01 | Item 01)

ESCOPO DA SOLUÇÃO:

Os detalhamentos técnicos das infraestruturas abaixo esboçadas e a metodologia da execução de seu fornecimento serão descritos em suas especificidades técnicas neste Termo de Referência.

DESCRIÇÃO:

* + 1. Serviço de Storage em nuvem Storage Mínimo Requerido:
    2. 10 Tbytes em Storage redundante e clusterizado, sendo:
    3. 8 Tb em HDD SAS/SATA;
    4. 2 Tb em SSD.
    5. Serviço de Computação em nuvem, sendo:
    6. 40 unidades de VCPU com processadores mínimos de 2.1 Ghz;
    7. 256 Gb de memória RAM DDR4;
    8. Conexão de Interligação (Transporte)
    9. Mínimo de 1 Gb/s;
    10. SLA 99,00% de disponibilidade;
    11. Serviços de Suporte e Manutenção 24x7x365
    12. Gerenciamento de Continuidade
    13. ESPECIFICIDADES TÉCNICAS EXIGIDAS
    14. STORAGE:
    15. Storage deve ser de linha enterprise, não serão aceitas soluções opensource ou OEM.
    16. Deve funcionar em modo clusterizado com duas controladoras ativas-ativas.
    17. Deve possuir no mínimo 7GB de cache somando as duas controladoras com no mínimo 32GB de ram em cada uma.
    18. Todos os discos do storage devem ser homologados pelo fabricante do equipamento.
    19. O sistema de storage deve prover funcionalidades como thinprovisioning e snapshots integrada. A funcionalidade de snapshot do sistema de storage deve ser homologada pela solução de backup para prover restauração de arquivos e tabelas de bancos de dados SQL dentro das vms e outros através dos snapshots de storage de forma integrada com a solução de backup apresentada. Essa funcionalidade deve ser comprovada com o datashet indicando a integração de ambas.
    20. O Gerenciamento do storage deve ser homologado para a versão maior mais recente do vmware.
    21. Deve ser entregue 8 TB de armazenamento em discos SAS utilizável e 2 TB de armazenamento em SSD enterprise utilizável com suporte à gravação intensiva, todos homologados pelo fabricante da solução de storage.
    22. Devem ser validadas as informações apresentadas no folder com o armazenamento já presente no storage. Pode ser realizado via acesso remoto.
  1. VIRTUALIZAÇÃO:
     1. O Ambiente de Virtualização deve possuir processadores com no mínimo 2.0Ghz, cache de 23MB total, 10 Cores e 20 Threads. Suporte à memória DDR4. Litografia mínima de 14 nm.
     2. Não serão aceitas soluções OEM.
     3. Não serão aceitas soluções incompatíveis com arquitetura de servidores.
     4. As memória do ambiente de virtualização deve ser de no mínimo 256GB de RAM DDR4 ECC.
     5. O sistema de virtualização deve estar instalado em SSD de no mínimo 128GB.
     6. Os hosts devem ser homologados para funcionar com a versão maior mais atual do Vmware.
     7. A conectividade de rede para vms e entre o storage e servidores deve ser do no mínimo 20Gb cada uma.
     8. Devem ser validados com ambiente acessado remotamente comprovando as informações presentes nos folders e prospects.
     9. Pode ser realizado via acesso remoto.
  2. INTERLIGAÇÃO:
     1. A interligação deve ser de alta disponibilidade com velocidade mínima de 1Gb/s (1 gigabits por segundo) entre o datacenter e a Câmara Municipal de Itaúna.
     2. Deve ter uma latência máxima de 11ms.
     3. QUANTO AO ANS (ACORDO DE NÍVEL DE SERVIÇOS):
     4. A solução como um todo deve ter um ANS (acordo de nível de serviço), total de 99,00% de disponibilidade mensurada mensalmente.
     5. Em caso de descumprimento da ANS em qualquer item será descontado do valor da parcela a ser paga o valor de 5% da parcela corrente para cada 0,1% de indisponibilidade de QUALQUER ITEM do ambiente (a saber, INTERLIGAÇÃO, VIRTUALIZAÇÃO, STORAGE, REDE, SISTEMA DE GERENCIAMENTO DE CONTINUIDADE).
     6. A CONTRATANTE se reserva o direito de cancelar o contrato sem nenhum ônus em caso do ANS mensal baixar para menos de 98% somadas todas as ocorrências no mês corrente.
     7. Em caso de cancelamento de contrato será repassada para a próxima colocada e a migração ocorrerá dentro do prazo de um mês sem ônus para a CONTRATANTE.
     8. O ANS será calculado a partir de comunicação da Câmara com a CONTRATADA por qualquer meio disponibilizado (telefone, whattsapp e/ou sistema de chamados) e será considerada pausada a partir da confirmação da cessação do problema por parte da CONTRATANTE.
     9. Em caso de degradação de performance de qualquer item (a saber, INTERLIGAÇÃO, HOSTS, STORAGE, REDE), sem paralisação de serviços será considerada a mesma métrica do ANS de parada de ambientes acima, com a exceção da média mensal que pode ficar em 95% mensurada mensalmente. Em caso de descumprimento do ANS durante 3 vezes por semestre, será contabilizado como passível de cancelamento de contrato e posterior punição pela CONTRATANTE.
  3. QUANTO AO AMBIENTE DE VIRTUALIZAÇÃO
     1. O ambiente de virtualização deve funcionar isolado de qualquer outro ambiente que não seja da CONTRATANTE, deve ser configurado com o Vmware no mínimo na versão 7U3.
     2. O licenciamento do vmware é de responsabilidade da CONTRATADA.
     3. A configuração do vmware deve ser indicada pelo CONTRATANTE e ficará a cargo da CONTRATADA fazê-lo seguindo as melhores práticas recomendadas pelo fabricante.
     4. QUANTO AO SUPORTE E MANUTENÇÃO
     5. A CONTRATADA pode, através de comunicação com uma semana de antecedência (e devido aceite por parte do TI da CONTRATANTE), realizar 1 (UMA) manutenção agendada mensalmente para atualizar os sistemas fora do horário comercial (segunda a sexta das 7h-19h e sábado das 7h-16h).
     6. A CONTRATADA deve prover contato telefônico e sistema de chamados 24x7 para emergências e aberturas de chamados.
     7. A CONTRATADA deverá prover profissionais qualificados em todo o ambiente (VMWARE, INTERLIGAÇÃO, INTERNET, STORAGE, HOSTS, REDE, BACKUP CLOUD) para suporte 24x7x365 a todo o ambiente através de telefone.
     8. O suporte deverá ser prestado por profissionais nível 3 (especializados) em todo o processo desde a abertura do chamado. A abertura de chamados para questões que não envolvam degradação de performance do ambiente e/ou indisponibilidade de ambiente deverão ser feitas através de abertura de chamados no sistema de tickets.
     9. O sistema de chamados deverá seguir os padrões da ITIL (v2 ou v3) nos seus processos.
     10. O suporte deverá cumprir um Acordo de Nível de Serviços conforme o item ANS acima e também conforme a classificação abaixo:
     11. Dúvidas e questões sem impacto ao ambiente: 48 horas corridas após abertura do chamado para resolução.
     12. Mudanças de configurações sem indisponibilidade atual: 12 horas corridas após abertura do chamado.
     13. Demais atendimentos de maior criticidade devem ser resolvidos em até 8 horas obedecendo ao ANS de indisponibilidade de ambientes. Essas horas de resolução não podem ser contabilizadas como atenuantes da ANS de indisponibilidade ou perda de desempenho.
     14. Em caso de descumprimento do ANS durante 12 vezes por semestre, será contabilizado como passível de cancelamento de contrato e posterior punição pela CONTRATANTE.
  4. QUANTO ÀS QUALIFICAÇÕES TÉCNICAS
     1. A empresa CONTRATADA deve ter em seu corpo técnico, profissionais qualificados nas soluções de backup, alta disponibilidade e virtualização propostas. Também deverá ser apresentado neste processo junto com toda a documentação, o(os) Atestado de capacidade técnica que demonstre(m) entrega de solução em computação em nuvem. Outro atestado de capacidade técnica que demonstre a solução de backup e continuidade de negócios ofertada com quantidade mínima de 50% da quantidade ofertada. Podem ser usados múltiplos atestados para conseguir a quantidade pretendida na solução de continuidade.
  5. Backup Empresarial (Lote 01 | Item 02)
     1. A solução ofertada deverá, obrigatoriamente, atender as especificações mínimas previstas neste termo quanto às funcionalidades, integrações e compatibilidades com o ambiente virtualizado da CONTRATANTE para criação de backups e recuperação desses ambientes com o mínimo de indisponibilidade e reestruturação da parte física necessária, de forma que recupere, total e/ou granular, qualquer item assegurado por sua funcionalidade de backup e restauração.
     2. Deverá ser fornecido licenciamento do software, em caráter de aluguel de licenças, de propriedade e registrado para a CONTRATANTE, na modalidade de capacidade por quantidade de máquinas virtuais (VMS) para o ambiente virtualizado e por quantidade de servidores (hosts) para o ambiente físico, com suporte para backup e restore de dados.
     3. Cada licença de software licenciará UM TOTAL DE 30 VMS, do ambiente virtualizado (provedor/host das máquinas virtuais) e também físico da CONTRATANTE.
     4. Não poderão ser limitadas pelo volume de dados movimentados pelos mesmos.
     5. Deverá incluir funcionalidades de proteção (backup) e replicação integradas em uma única solução.
     6. Não deverá necessitar de instalação de agentes para poder realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais.
     7. Deverá garantir, no mínimo, a proteção de máquinas virtuais e seus dados, gerenciadas através das soluções de virtualização VMware ou HYPER-V.
     8. Deverá ter a capacidade de replicação de dados armazenados entre storages ou máquinas de configuração e de fabricantes diferentes.
     9. Deverá proteger o ambiente, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção (backup) e migrações em conjunto.
     10. Deverá ter a capacidade de testar a consistência do backup e replicação (S.O., aplicação, VM), emitindo relatório de auditoria para garantir a capacidade de recuperação.
     11. Deverá prover a deduplicação e compressão durante a operação de qualquer backup sem a necessida - de de hardware de terceiros (appliance deduplicadora).
     12. Deverá possibilitar a cópia de uma máquina virtual completa ou discos virtuais específicos.
     13. Deverá ser fornecida com ferramenta de gestão de arquivos para os administradores de máquinas virtuais no console do operador.
     14. Deverá ter a capacidade de integração através de API’s dos fabricantes de infraestrutura virtualizada para a proteção de dados.
     15. Deverá ter a capacidade de realizar proteção (backup) incremental e replicação diferencial, aproveitando a tecnologia de “rastreio de blocos modificados” (CBT – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e possibilitando proteção (backup e replicação).
     16. Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup), a saber:
         1. Diretamente através de Storage Area Network (SAN);
         2. Diretamente do storage, através do hypervisor I/O (Virtual Appliance);
         3. Mediante uso da rede local (LAN);
         4. Diretamente do snapshot do storage onde os dados das VMs estejam armazenados;
     17. Deverá manter um backup sintético, eliminando assim a necessidade de realizar backups completos (full) periódicos, incremental permanente, o que permitirá economizar tempo e espaço.
     18. Deverá possibilitar a inicialização de uma máquina virtual diretamente do arquivo de backup, inclusive sem necessidade de “hidratação” dos dados “deduplicados e “comprimidos”.
     19. Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.
     20. Todo serviço de migração das máquinas virtuais do repositório de backup até o armazenamento na produção restabelecida não deverá afetar a disponibilidade e acesso pelo usuário, sem paradas.
     21. Deverá prover acesso ao conteúdo das máquinas virtuais, para recuperação de arquivos, pastas ou anexos, diretamente do ambiente protegido (repositório de backup) ou replicados, sem a necessidade de recuperar completamente o backup e inicializar uma máquina virtual.
     22. Deverá permitir realizar buscas rápidas mediante os índices dos arquivos que sejam controlados por um sistema operacional Windows, quando este seja o sistema operacional executado dentro da máquina virtual da qual se tenha realizado o backup.
     23. Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
     24. Deverá permitir realizar a truncagem de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, SQL Server e Oracle.
     25. Deverá permitir notificações por correio eletrônico, SNMP ou através dos atributos da máquina virtual do resultado da execução de seus trabalhos.
     26. Deverá permitir recuperar no nível de objetos e arquivos de qualquer aplicação virtualizada, em qualquer sistema operacional, utilizando as ferramentas de gestão das aplicações existentes.
     27. Deverá incluir ferramentas de recuperação sem a necessidade de agentes, sem a necessidade de recuperar os arquivos da máquina virtual como um todo ou reiniciar a mesma (recuperação granular), para os servidores:
     28. Microsoft Exchange 2016, possibilitando recuperar objetos individuais, tais como contatos, mensagens, compromissos, anexos, entre outros.
     29. Microsoft Active Directory 2016, possibilitando recuperar objetos individuais, tais como usuários, recuperaçăo de senhas de usuários e computadores, grupos, contas, Objetos de Política de Grupo (GPOs), registros do Microsoft DNS integrados ao Active Directory entre outros sem a necessidade de usar o agente tanto para backup e restauração.
     30. Microsoft SQL Server 2014 ou superior, possibilitando recuperar objetos individuais, tais como bases, tabelas, registros, entre outros; Microsoft Sharepoint 2016.
     31. Deverá oferecer testes automatizados de recuperação para todas as máquinas virtuais protegidas, garantindo a confiabilidade na execução correta das máquinas virtuais e de suas aplicações (DNS Server, Controlador de domínio, Servidor de e-mail, etc.), no momento da recuperação.
     32. Deverá ser possível executar uma ou várias máquinas virtuais a partir do arquivo de backup, em um ambiente isolado de forma automática através de schedule, sem a necessidade de espaço de armazenamento adicional e sem modificar os arquivos de backup (read-only), para criação de ambiente de homologação, teste, etc.
     33. Deverá oferecer arquivamento em fita, suportando VTL (Virtual Tape Libraries), biblioteca de fitas e drives LTO5 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia GFS, sem a necessidade de licenciamento individual por drive;
     34. Deverá oferecer trabalhos de cópia de backup com implementação de políticas de retenção.
     35. Deverá operar em ambientes virtualizados através das soluções da Vmware, incluindo: VMware vSphere 7.
     36. Deverá garantir a recuperação granular e consistente, sem necessidade de instalação de agentes adicionais para o ambiente virtualizado através das soluções acima, principalmente para os seguintes softwares:
         1. Microsoft Active Directory 2016;
         2. Microsoft Exchange Server 2016;
         3. Microsoft Sharepoint 2013 ou superior
         4. Oracle Database 12 ou superior.
     37. Deverá ser capaz de realizar réplicas em outros sites ou infraestruturas a partir dos backups realizados.
     38. Deverá regular de forma dinâmica e parametrizável, o uso de recursos computacionais, de forma que se possa diminuir o impacto na infraestrutura de produção, durante as atividades de backup.
     39. Deverá permitir um método de fácil de recuperação, desde ambientes de contingência, com as ações pré-configuradas para evitar ações manuais em caso de desastre, similar a um botão de emergência.
     40. Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo de 256 bits, ativando e desativando tal operação, assim como assegurar o trânsito da informação através desse cenário.
     41. Deverá permitir a criação de níveis de delegação de tarefas (perfis) de recuperação no nível de ele - mentos da aplicação, inclusive para outros usuários, de forma a diminuir a carga de atividades executadas pelo administrador da plataforma.
     42. Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo:
     43. Relatórios que permitam o planejamento de capacidade.
     44. Relatórios que permitam determinar a ineficiência dos recursos em uso.
     45. Relatórios que facilitem a visibilidade de tendências negativas e anomalias.
     46. Quadros de controle claros, apresentáveis e integráveis em sites web.
     47. A licença de software de Backup deverá, nativamente, ser capaz de emitir relatórios com informações completas, conforme subitens:
     48. Permitir acesso aos relatórios através de interface gráfica ou web.
     49. Suportar a geração de relatórios gráficos customizáveis de atividades de backups/restores, contendo: Horário de início e término dos jobs; Tempo de duração dos jobs; Todos os jobs em execução; Status (situação) de execução dos jobs; Relação e porcentagem de jobs executados por status, como por exemplo: com sucesso e com erros; Logs dos jobs; Volume de dados na origem e no destino, total e por job, por período de tempo, por localidade e por host (físico ou virtual); Tendência de crescimento; Dados históricos de, no mínimo, 24 (vinte e quatro) meses.
     50. Suportar a geração de relatórios gráficos customizáveis de atividades de backups, contendo: Identificação da ocupação nos destinos de backups: uso de disco e fita; Porcentagem de dados deduplicados; Taxa de deduplicação e compressão.
     51. Permitir a geração de relatórios baseados na utilização de recursos, identificando restrições associa - das a aplicativos específicos.
     52. Permitir a geração de relatórios baseados em alertas pré-definidos, com o objetivo de reportar even - tos ocorridos do ambiente operacional de backup e restore.
     53. Deverá correlacionar a execução de trabalhos de backup e réplica com os objetos do ambiente virtual.
     54. Deverá oferecer a capacidade de relatar o cumprimento das políticas de proteção de dados e disponibilidade de acordo com parâmetros definidos.
     55. Deve suportar múltiplas operações dos componentes/servidores participantes da estrutura de backup, permitindo atividades de backup e recuperação simultâneas.
     56. Deve suportar repositório de backup com aumento de escala ilimitado para o armazenamento de dados com suporte aos seguintes sistemas de armazenamento:
         1. Microsoft Windows;
         2. Linux;
         3. Pastas compartilhadas;
         4. Appliances deduplicadoras.;
         5. Storages do tipo SAN e NAS.
         6. Nuvem (Amazon AWS, Microsoft Azure).
     57. Deverá permitir a seleção de um destino de armazenamento do backup em um provedor de serviços em nuvem (BaaS – Backup as a Service).
     58. Deverá permitir a seleção de um destino para a réplica dos dados que poderá ser em um provedor de serviços em nuvem (DRaaS – DR as a Service).
     59. Possuir integração com armazenamento de objetos compatíveis com S3 como Amazon S3, Azure Blob Storage e qualquer outro dispositivo de armazenamento local compatível com S3.
     60. Realizar arquivamento dos dados de backup nos dispositivos e locais de armazenamento de objetos compatíveis com S3.
     61. Em caso de desastre, deverá ser possível realizar a recuperação dos dados diretamente do arquivamento em S3.
     62. A solução deverá possuir integração com soluções de antivírus de modo a realizar uma varredura de segurança nos dados de backup antes de realizar sua recuperação.
     63. Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem.
     64. Deve ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, o CONTRATANTE se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional.
     65. Deve ser ofertada junto com a solução o armazenamento de 20 tb de dados em ambiente de cloud computing isolado do ambiente ofertado para a CÂMARA com suporte integrado à solução para backup dos dados, com proteção dentro da interface de gerenciamento da solução para evitar “inside atacks” (ataques que objetivam o backup e a deleção dos mesmos). O ambiente de nuvem deve ser integrado para permitir a partir de uma interface única desenvolver tanto o backup quanto o restore de todo o ambiente.
     66. O software de backup irá rodar dentro do ambiente da CONTRATANTE e será configurado seguindo as melhores práticas do mercado pela CONTRATADA. A utilização do mesmo será de responsabilidade da CONTRATANTE no dia a dia e em caso de necessidade será acionada a CONTRATADA para dirimir dúvidas e realizar configurações mais especializadas.
  6. Antivírus (Lote 01 | Item 03)
     1. REQUISITOS MÍNIMOS PARA A SOLUÇÃO DE ANTIVÍRUS
        1. Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos, controle de aplicações e criptografia de discos.
        2. A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento, e caso não tenha a capacidade de realização a remoção completa, a contratada deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual;
        3. O produto deverá possuir no mínimo os seguintes módulos e funcionalidades:
        4. Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas;
        5. Módulos para estações físicas, notebooks e servidores;
        6. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;
        7. Módulo para dispositivos móveis no mínimo para tablets e smartphones com sistema operacional iOS e Android; (Somente em console On-premise).
        8. Utilizar o conceito de heurística para combate e ações contra possíveis malwares.
        9. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit).
        10. Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware.
        11. Oferecer inventário de softwares.
        12. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção.
        13. Oferecer proteção por base de assinaturas (vacinas).
     2. CONSOLE DE GERENCIAMENTO
        1. Instalação e configuração
        2. Permitir instalação de console local (on-premise) com banco de dados local ou instalação em nuvem (cloud) com banco de dados também em nuvem.
        3. Para a opção de console local de ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo as seguintes plataformas de virtualização:
           1. VMWare vSphere;
           2. Citrix XenServer; XenDesktop, VDI-in-a-Box;
           3. Microsoft Hyper-V;
           4. Red hat Enterprise Virtualization;
           5. Kernel-based Virtual Machine ou KVM;
           6. Oracle VM;
        4. Deverá ser fornecido com base de dados embutida e proprietária ou com possibilidade de utilização de banco de dados externo SQL ou Oracle;
        5. Para instalação da console em nuvem (cloud), a nuvem deve ser privada e do mesmo fabricante.
        6. Permitir instalação remota via console WEB de gerenciamento para ambientes virtuais VMWare ou Citrix.
        7. O mecanismo de varredura deverá estar disponível para download separadamente.
        8. A solução deverá permitir a inclusão de um modulo de balanceamento para casos em que vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance, dentre outras necessidades).
        9. Deve ser totalmente em português.
     3. Funcionalidades Gerais:
        1. Licenciamento flexível;
        2. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações:
           1. Nome;
           2. IP;
           3. Sistema Operacional;
           4. Política Aplicada;
           5. Usuário logado (se disponível).
        3. A console de gerenciamento deverá incluir sessão de log com as seguintes informações:
           1. Login;
           2. Edição;
           3. Criação;
           4. Log-out;
        4. Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas funções e serviços da solução.
        5. Permitir que o administrador escolha qual o pacote será atualizado.
        6. As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail.
        7. No mínimo enviar notificações para as seguintes ocorrências:
           1. Problemas com licenças;
           2. Alertas de surto de vírus;
           3. Máquinas desatualizadas;
           4. Eventos de antimalware.
        8. Deverá prover o acesso via HTTPS.
        9. Deverá permitir a importação de certificados digitais.
        10. O gerenciamento e a comunicação com dispositivos móveis devem ser feitos de forma segura utilizando certificados digitais.
     4. Monitoramento:
        1. Baseado em “portlets” configuráveis com no mínimo as seguintes especificações:
           1. Nome;
           2. Tipo de relatório;
           3. Alvo do relatório;
        2. Deverá disponibilizar “portlets” para gerência e monitoramento de qualquer tipo de endpoint, máquinas físicas, virtuais e dispositivos móveis.
        3. Inventário da Rede
        4. Possuir no mínimo as integrações abaixo:
           1. Múltiplos domínios do Active Directory;
           2. Múltiplos VMWare vCenters;
           3. Múltiplos Citrix Xen Servers;
        5. Possuir a possibilidade de definição de sincronização com o Active Directory em horas.
        6. Descoberta de rede para máquinas em grupo de trabalho.
        7. Possuir busca em tempo real pelo menos com os seguintes filtros:
           1. Nome;
           2. Sistema Operacional;
           3. Endereço IP;
        8. Possibilitar a instalação remota e desinstalação remota do antivírus.
        9. Possibilitar a configuração de pacotes de instalação do produto de antivírus.
        10. Possuir tarefas remotas e configuráveis de scan.
        11. Possuir tarefa de reinicialização remota de estação ou servidor.
        12. Assinar políticas para no mínimo os níveis:
            1. Computador;
            2. Máquina Virtual;
            3. Grupo de Endpoints;
            4. Usuário do AD;
            5. Localização lógica da máquina;
            6. Grupo do AD.
        13. Possuir a propriedade detalhada de objetos gerenciados para:
            1. Nome;
            2. IP;
            3. Sistema Operacional;
            4. Grupo;
            5. Política Assinada;
            6. Ultimo status de malware.
     5. Políticas
        1. Modelo único para todos os equipamentos, sejam físicos ou virtuais.
        2. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar.
        3. Através da console de gerenciamento o administrador poderá ser capaz de enviar uma política única para configurar o antivírus.
        4. Deverá configurar as funcionalidades como escaneamento do antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, criptografia (Windows, Mac e Android), localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade.
     6. Relatórios
        1. Deverá apresentar as seguintes funcionalidades:
           1. Relatório para cada serviço de segurança;
           2. Facilidade de usar e visualização simplificada;
           3. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;
           4. Filtros de agendamento de relatórios;
           5. Arquivo com todas as instâncias de relatório agendados;
           6. Exportar o relatório nos formatos .pdf e/ou .csv;
           7. Oferecer possibilidade de criar relatórios de maneira dinâmica no dashboard da da console de gerenciamento.
     7. Administração de Usuários
        1. Deverá apresentas no mínimo as seguintes funcionalidades:
           1. Administração baseada em regras;
           2. Disponibilizar tipos de usuários pré-definidos como no mínimo:
           3. Administrador – Gerente dos componentes da solução;
           4. Administrador de rede - Gerente dos serviços de segurança;
           5. Relatório – Monitora e cria relatórios;
           6. Deverá ser possível customizar um tipo de usuário:
           7. Deverá permitir a integração de usuários com o Active Directory para autenticação da console de gerenciamento;
           8. Registrar as ações do usuário na console de gerenciamento;
           9. Detalhar cada ação do usuário;
           10. Permitir busca complexa baseada em ações do usuário, intervalos de tempo.
     8. SEGURANÇA PARA ESTAÇÕES E SERVIDORES
        1. Proteção para ambientes físicos
        2. Deverá proteger em tempo real e agendado as máquinas físicas em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto na console local (on-premises) como na console em nuvem (cloud);
        3. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:
           1. Windows 10 64Bits;
           2. Windows 8.1 64Bits;
           3. Windows 8 64Bits;
           4. Windows 7 64Bits;
        4. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:
           1. Windows Server 2012R2;
           2. Windows Server 2012;
           3. Windows Server 2008 R2;
        5. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux:
           1. Ubuntu 14.04 LTS ou superior
           2. Red Hat Enterprise Linux / CentOS 6 ou superior
           3. SUSE Linux Enterprise Server 11 SP4 ou superior
           4. OpenSUSE Leap 42.x
           5. Fedora 25 ou superior
           6. Debian 8.0 ou superior
           7. Oracle Linux 6.3 ou superior
           8. Amazon Linux AMI 2016.09 ou superior
           9. Proteção para ambientes virtuais
        6. Para plataforma de virtualização com VMWare, deverá:
           1. Ter a disponibilidade de ser integrado e oferecer a escaneamento sem instalar o agente nas máquinas virtuais;
           2. A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;
           3. Deverá proteger em tempo real e agendado as máquinas virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto no console local (on-premises) como na console em nuvem (cloud);
        7. O produto deverá oferecer agente para virtualização dos seguintes produtos:
           1. Citrix Xen Server;
           2. Microsoft Hyper-V;
           3. VMware ESXi;
           4. Red Hat Virtualization;
           5. Oracle KVM;
           6. KVM.
     9. Instalação e Configuração Remota
        1. Deverá permitir ao administrador customizar a instalação;
        2. Deverá permitir a instalação customizada do antivírus com no mínimo:
           1. Instalar o antivírus sem o controle de acesso a internet; (Windows Desktop)
           2. Instalar o antivírus sem o módulo de firewall; (Windows Desktop)
        3. A instalação deverá ser possível executar com no mínimo das seguintes maneiras:
           1. Executar o pacote de antivírus diretamente na estação de trabalho;
           2. Instalar remotamente, distribuído via console de gerencia web;
           3. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;
           4. Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;
           5. Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;
           6. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário a distribuição em um agente separado.
     10. Funções Gerais
         1. Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança;
         2. Deverá permitir a configuração do scan do antivírus do cliente como:
            1. Scan local;
            2. Scan hibrido (local\remoto);
            3. Scan remoto;
         3. Deverá reportar o estado atual das máquinas virtuais no mínimo, protegida/desprotegida;
         4. Deverá fazer scan em tempo real e automático;
         5. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;
         6. Deverá possuir escaneamento baseado em análise heurística;
         7. Deverá permitir a escolha e configuração de pastas a serem scaneadas;
         8. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção:
            1. Baseada em assinaturas;
            2. Baseada em heurística;
            3. Baseada em monitoramento contínuo de processos;
         9. Módulo de Antiexploit disponível para servidores e estações de trabalho baseado em Machine Learning para proteger contra vulnerabilidades de softwares;
         10. Deve possuir módulo de mitigação de Ransomware para detecção e recuperação de possíveis arquivos criptografados.
         11. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho;
         12. O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor nas estações de trabalho;
         13. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;
         14. No módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;
         15. Deve possuir módulo de proteção contra ataques de rede que fornece uma camada de segurança a mais que detecta e executa ações contra ataques de rede projetados para obter acesso em endpoints através de técnicas específicas, tais como: ataques de força bruta, explorações de rede, ladrões de senha, movimentação lateral, etc
         16. Deverá ter os seguintes requisitos mínimos de sistema:
             1. Plataformas de Virtualização
             2. VMware vSphere ESX 5.0 ou superior;
             3. VMware vCenter Server 4.1 ou superior;
             4. Citrix XenDesktop 5.0 ou superior;
             5. Xen Server 5.5 ou superior;
             6. Citrix VDI-in-a-Box 5;
             7. Microsoft Hyper-V Server 2008 R2, 2012
             8. Oracle VM 3.0;
             9. Red Hat Enterprise Virtualization 3.0.
             10. Sistemas Operacionais para Desktops
             11. Windows 10 64Bits;
             12. Windows 8.1 64Bits;
             13. Windows 8 64Bits;
             14. Windows 7 64Bits;
             15. Sistemas Operacionais para Servidores
             16. Windows Server 2012R2;
             17. Windows Server 2012;
             18. Windows Server 2008 R2;
             19. Windows Server 2008 apenas os módulos de antivírus e Active Virus Control;
             20. Linux Red Hat Enterprise;
             21. CentOS 5.6 ou superior;
             22. Ubuntu 10.04 LTS ou superior;
             23. SUSE Linux Enterprise Server 11 ou superior;
             24. OpenSUSE 11 ou superior;
             25. Fedora 15 ou superior;
             26. Debian 5.0 ou superior.
     11. Quarentena
         1. Deverá permitir restauração remota, com configuração de localidade e deleção;
         2. Criação e exclusão para arquivos restaurados;
         3. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;
         4. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
         5. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
         6. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
         7. Deverá permitir escanear a quarentena após a atualização de assinaturas.
     12. Controle de Usuário
         1. Deverá ter módulo de controle de usuário integrando com as seguintes características:
            1. Bloqueio de acesso a internet;
            2. Bloqueio de acesso a aplicações definidas pelo administrador.
     13. Controle do Dispositivo
         1. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
         2. Através do módulo de controle de dispositivo deverá ser possível controlar:
            1. Bluetooth;
            2. CDROM/DVDROM;
            3. IEEE 1284.4;
            4. IEEE 1394;
            5. Windows Portable;
            6. Adaptadores de Rede;
            7. Adaptadores de rede Wireless;
            8. Discos Externos;
         3. Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:
            1. CD/DVD;
            2. Discos Externos;
            3. Pen-Drivers;
         4. Deverá permitir regras de definição de bloqueio/desbloqueio;
         5. Deverá permitir regras de exclusão.
     14. Criptografia
         1. Deverá oferecer:
            1. Possibilidade de criptografia de disco através da mesma console de gerenciamento do antivírus, seja em nuvem (cloud) ou local (on-premise);
            2. Deverá utilizar quando necessário serviços de criptografia com agentes nativos da estação de trabalho seja baseada em Windows ou Mac;
            3. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
            4. Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra.
     15. Atualização
         1. Após a atualização o administrador deverá ter a capacidade de configurar uma reinicialização;
         2. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
         3. Permitir atualizações de assinatura de hora em hora;
         4. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.
  7. Acces Point Corporativo (Lote 01 | Item 04 )
     1. ESPECIFICAÇÕES:
        1. Networking porta de interface ethernet: (1) 10/100/1000
        2. Botões de reset
        3. Temperatura operacional -30 a 60 °c (-22 a 140 °f)
        4. Umidade de operação 5 a 95%, sem condensação
        5. Certificações ce, fcc, ic
        6. Segurança sem fio: wep, wpa - bssid: até quatro por
     2. ALIMENTAÇÃO DE ENERGIA:
        1. Método de energia: poe 802.3af, poe passivo (48v)
        2. Fonte de energia: 802.3af poe 48v, adaptador poe 0,32a (opcional)
        3. Faixa de tensão suportada: 44 a 57vdc
        4. Consumo de energia: máxima 12w
     3. POTÊNCIA MÁXIMA TX:
        1. 2.4 ghz: 23 dbm
        2. 5 ghz: 17 dbm
     4. ANTENAS:
        1. Dual-band
        2. 2.4 ghz: 2,8 dbi
        3. 5 ghz: 3dbi
        4. Wi-fi padrões: 802.11 a / b / g / n / ac
     5. MONTAGEM:
        1. Na parede / teto (kits incluídos)
     6. GERENCIAMENTO DE TRÁFEGO AVANÇADO:
        1. Padrões de wifi: 802.11a / b / g | wifi 4 / wifi 5 / wifi 6
        2. Segurança sem fio: wpa-psk, wpa-enterprise (wpa / wpa2 / wpa3)
        3. Bssid: 8 por rádio
        4. Vlan: 802.1q
        5. Qos avançado: limitação de taxa por usuário
        6. Isolamento do tráfego de visitantes: suportado
        7. Clientes simultâneos: 300+
        8. Gerenciamento centralizado via máquina virtual
     7. TAXAS DE DADOS SUPORTADAS (MBPS):
        1. TAXAS PADRÃO
        2. 802.11A: 6, 9, 12, 18, 24, 36, 48, 54 MBPS
        3. 802.11B: 1, 2, 5,5, 11 MBPS
        4. 802.11G: 6, 9, 12, 18, 24, 36, 48, 54 MBPS
        5. 802.11N: (WIFI 4) 6,5 MBPS A 300 MBPS (MCS0 - MCS15, HT 20/40)
        6. 802.11AC: (WIFI 5) 6,5 MBPS A 866,7 MBPS (MCS0 - MCS9 NSS1 / 2, VHT 20/40/80)
        7. 802.11AX: (WIFI 6) 7,3 MBPS A 1,2 GBPS (MCS0 - MCS11 NSS1 / 2, HE 20/40/80)
     8. Controladora Fisica:
     9. Interfaces Networking:
        1. 8x Portas LAN RJ45 10/100/1000
        2. 1x 10/100/1000 Porta WAN RJ45
        3. 1x Porta 1 / 10G SFP + LAN
        4. 1x 1 / 10G SFP + Porta WAN
     10. Gestão:
         1. Ethernet em banda
         2. 1x Bluetooth BLE
     11. Taxa de transferência de IDS / IPS:
         1. 3,5 Gbps \*
     12. Processador:
         1. Quad ARM Cortex-A57 Core a 1,7 GHz
     13. Memória do sistema:
         1. 4 GB DDR4
     14. Armazenamento Flash On-Board:
         1. 16 GB eMMC
     15. Consumo máximo de energia:
         1. 33W
     16. Alcance de voltagem:
         1. 100 a 240VAC
     17. Método de energia:
         1. 1x Entrada CA universal, 100-240 VCA, 50/60 Hz
         2. 1x Entrada RPS DC
  8. Firewall (Lote 01 | Item 05)
     1. 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, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico ou virtualizado.
     2. Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / *malwares, endpoints, softwares de criptografia de armazenamento em nuvem* e assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período mínimo de 36 (trinta e seis) meses.
     3. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos em caráter de locação pelo período de 12 messes.
     4. Por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.
     5. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
     6. A *appliance* deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.
  9. CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DO FIREWALL DE PRÓXIMA GERAÇÃO TIPO 1
     1. Performance mínima de 10.500 Gbps de throughput para firewall.
     2. Performance mínima de 2 Gbps de throughput de IPS.
     3. Performance mínima de 685 Mbps de throughput para controle de Threat Protection.
     4. Performance mínima de 1.8 Gbps de throughput de VPN.
     5. Suporte a, no mínimo, 1.600.000 de conexões simultâneas.
     6. Suporte a, no mínimo, 61.500 novas conexões por segundo.
     7. Possuir o número irrestrito quanto ao máximo de usuários licenciados.
     8. Possuir armazenamento interno de no mínimo 64 GB SSD para sistema operacional, quarentena local, logs e relatórios.
     9. Possuir no mínimo 8GB de memória RAM.
     10. Possuir no mínimo 8 (oito) interfaces de rede 1000Base-TX.
     11. Possuir no mínimo 1 (uma) interfaces SFP
     12. Possuir 1 (uma) interface do tipo console ou similar.
  10. CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO TIPO
      1. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência, monitoração e logs.
      2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
      3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.
      4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
      5. O software deverá ser fornecido em sua versão mais atualizada.
      6. O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.
      7. O hardware deve ser do mesmo fabricante do software, não sendo aceitas soluções OEM.
      8. Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.
      9. A atualização de software deverá enviar avisos de atualização automáticos.
      10. O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.
      11. O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.
      12. As notificações deverão ser realizadas via email e SNMP.
      13. Suportar SNMPv3 e Netflow.
      14. O firewall deverá ser stateful, com inspeção profunda de pacotes.
      15. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.
      16. As políticas de NAT deverão ser customizáveis para cada regra.
      17. A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS).
      18. Proteção contra anti-spoofing.
      19. Suportar IPv4 e IPv6.
      20. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.
      21. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).
      22. Deve possuir tecnologia de conectividade SD-WAN;
      23. Deve possibilitar o roteamento baseado em VPNs;
      24. Deve suportar criar políticas de roteamento
      25. Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:
      26. Interface de entrada do pacote;
      27. IPs de origem;
      28. IPs de destino;
      29. Portas de destino;
      30. Usuários ou grupos de usuários;
      31. Aplicação em camada 7.
      32. Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento.
      33. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.
      34. Deve suportar Extended VLAN.
      35. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.
      36. 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.
      37. Deve permitir a configuração de jumbo frames nas interfaces de rede.
      38. Deve permitir a criação de um grupo de portas layer2.
      39. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP.
      40. O traffic shapping (QoS) deverá ser baseado em rede ou usuário.
      41. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.
      42. Deve possuir otimização em tempo real de voz sobre IP.
      43. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
  11. CONTROLE POR POLÍTICAS DE FIREWALL
      1. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.
      2. 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.
      3. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.
      4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
      5. Controle de políticas por países via localização por IP.
      6. Suporte a objetos e regras IPV6.
      7. Suporte a objetos e regras *multicast*.
  12. PREVENÇÃO DE AMEAÇAS
      1. 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.
      2. Deve realizar a inspeção profunda de pacotes para prevensão de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).
      3. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.
      4. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras.
      5. 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.
      6. A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em núvem.
      7. Para a eficácia da análise de malwares Zero-Days, a solução de Sandobox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning.
      8. A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma.
      9. Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em núvem.
      10. A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.
      11. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.
      12. Deve ter proteção em tempo real contra novas ameaças criadas.
      13. 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.
      14. Deve permitir o bloqueio de vulnerabilidades.
      15. Deve permitir o bloqueio de *exploits* conhecidos.
      16. Deve detectar e bloquear o tráfego de rede que busque acesso a command and control e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.
      17. Deve incluir proteção contra ataques de negação de serviços.
      18. Ser imune e capaz de impedir ataques básicos como: *SYN flood, ICMP flood, UDP Flood*, etc.
      19. Suportar bloqueio de arquivos por tipo.
      20. 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.
      21. Os eventos devem identificar o país de onde partiu a ameaça.
      22. 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.
      23. O apliance deve ter a capacidade de atuar como um gateway antispam de modo que possa realizar filtragens dos emails e aplicar políticas.
      24. O gateway de email incluso no apliance deve ter pelo menos as seguintes proteções:
      25. Sender Policy Framework (SPF);
      26. Domain Keys Identified Mail (DKIM);
      27. Domain-based Message Authentication, Reporting & Conformance (DMARC);
      28. Bounce Address Tag Validation (BATV);
      29. O filtro de email deve quarentenar os emails suspeitos ou realmente maliciosos;
      30. A solução deve possibilitar aos usuários acessarem um painel para verificação da sua caixa pessoal de quarentena, possibilitando então a liberação ou a exclusão das mensagens;
      31. A função de antispam deve permitir a configuração de relays com a possibilidade de autenticação dos mesmos;
      32. A função de antispam deve possibilitar também o envio de emails seguros, realizando a criptografia das mensagens bem como dos seus anexos.
      33. A função de antispam deve conter funcionalidades de prevenção a perda de dados (DLP) para evitar que informações sigilosas sejam vazadas;
      34. O firewall de aplicação Web (WAF) deverá ter a função de reverse proxy, com a função de URL hardening realizando deep-linking e prevensão dos ataques de path traversal ou directory traversal.
      35. O firewall de aplicação Web (WAF) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.
      36. O firewall de aplicação Web (WAF) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parametros de performance do WAF e permissão e bloqueio de ranges de IP.
      37. 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.
      38. Proteção pelo menos contra os seguintes ataques, mas não limitado a: SQL injection e Cross-site scripting.
  13. CONTROLE E PROTEÇÃO DE APLICAÇÕES
      1. 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.
      2. Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3.
      3. O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os segiuntes algorítimos: curvas elipticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.
      4. O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não decriptografar, negar o pacote e criptografar para determinadas conexões criptografadas.
      5. Reconhecer pelo menos 2.300 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.
      6. 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 Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.
      7. 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).
      8. 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.
      9. Atualizar a base de assinaturas de aplicações automaticamente.
      10. Reconhecer aplicações em IPv6.
      11. Limitar a banda usada por aplicações (*traffic shaping*).
      12. 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.
      13. 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.
      14. 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.
  14. CONTROLE E PROTEÇÃO WEB
      1. 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.
      2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.
      3. 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.
      4. Autenticação em 2 fatores em conjunto com a autenticação Radius.
      5. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.
      6. Possuir pelo menos 90 categorias de URLs.
      7. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.
      8. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca.
      9. Deve ser capaz de forçar as restrições do Youtube.
      10. 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;
      11. Suportar a criação categorias de URLs customizadas;
      12. Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.
      13. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada
      14. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;
      15. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.
      16. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;
      17. Deve realizar caching do conteúdo web;
      18. Deve relizar filtragem por mime-type, extensão e tipos de conteúdos ativos, tais como, mas não limitado a: ActiveX, applets e cookies.
      19. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré determinados para acessar sites na internet.
      20. A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.
      21. Deve possuir capacidade de alguns usuários préviamente selecionados realizarem um bypass temporário na política de bloqueio atual.
      22. IDENTIFICAÇÃO DE USUÁRIOS
      23. 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.
      24. 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*).
      25. 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.
      26. 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.
      27. Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory e eDirectory.
      28. 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.
  15. QUALIDADE DE SERVIÇO - QoS
      1. 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.
      2. *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.
      3. 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.
      4. Suportar priorização *Real-Time* de protocolos de voz (VoIP).
      5. Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP;
      6. REDES VIRTUAIS PRIVADAS - VPN
      7. Suportar VPN *Site-to-Site e Cliente-to-Site*.
      8. Suportar IPsec VPN.
      9. Suportar SSL VPN.
      10. Suportar L2TP e PPTP.
      11. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.
      12. 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.
      13. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.
      14. Deve possuir opção de VPN IPSEC com client nativo do fabricante.
      15. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.
      16. 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).
      17. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Dell SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.
      18. 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.
      19. Suportar autenticação via AD/LDAP, *Token* e base de usuários local.
      20. Permitir estabelecer um túnel SSL VPN com uma solução de autienticação via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local.
  16. GERÊNCIA ADMINISTRATIVA CENTRALIZADA
      1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.
      2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
      3. Estar licenciada para gerenciar as soluções de firewall de próxima geração Tipo1.
      4. Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação.
      5. Deve ser centralizada a gerencia de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração Tipo1, sem necessidade de acesso direto aos equipamentos.
      6. Deve permitir a criação de Templates para configurações.
      7. Deve possuir indicadores do estado de equipamentos e rede.
      8. Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.
      9. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.
      10. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc).
      11. Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas.
      12. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.
      13. Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.
      14. Deve possibilitar o envio dos logs via syslog com conexão segura (TLS)
  17. GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS
      1. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.
      2. Estar licenciada para gerenciar as soluções de firewall de próxima geração Tipo1.
      3. Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 8TB de dados.
      4. Deverá prover relatórios baseados em usuários,com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.
      5. Deve possibilitar a identicação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.
      6. Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN.
      7. Deve fornecer relatórios históricos para análises de mudanças e comportamentos.
      8. Deve conter customizações dos relatórios para inserção de logotipos próprios.
      9. Deve fornecer relatórios de compliance SOX, HIPAA e PCI.
      10. Deve permitir a exportação via PDF ou Excel.
      11. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.
      12. Deve fornecer relatórios de tendências.
      13. Deve fornecer logs em tempo real, de auditoria e arquivados.
      14. Deve possuir mecanismo de procura de logs arquivados.
      15. Deve ter acesso baseado em Web com controles administrativos distintos.
  18. INTEGRAÇÃO COM SOLUÇÃO DE ENDPOINT
      1. A integração deve possibilitar a criação de regras de bloqueio de endpoints, com determinado status, dentro do Firewall de forma automática, sem que haja intervenção por parte do time da contratante.
      2. A integração deverá ser nativa entre o firewall e o endpoint, ou
      3. Utilizando APIs de integração da solução de firewall
      4. Caso a integração não seja nativa, cabe a CONTRATADA:
      5. Desenvolver completamente a solução de integração do Firewall e o Endpoint instalado (pelo menos Sophos Cloud).
      6. O Software de integração deve realizar a criação das regras do Firewall com no máximo 2 (dois) minutos após o incidente detectado no Endpoint.
      7. Possuir interface WEB, acessada por HTTP ou HTTPS, para definição dos objetos das regras a serem criados, com no mínimo origem, destino, status do endpoint e protocolos.
      8. Possibilitar o envio de emails sobre as ações do software.
  19. CONTRATO DE PRESTAÇÃO DE SERVIÇOS (Lote 01 | Item 06)
      1. A solução como um todo devera compor suporte Presencial + Remoto nos níveis N1,N2 e N3.
      2. O Suporte deverá cobrir todos os itens do Lote 1, como também deverá se estender a todos os ativos de rede já existentes na Câmara Municipal de Itaúna.
      3. A implantação configuração e manutenção dos itens que compõem o Lote 2, também ocorrera por conta da CONTRATADA.
      4. Suporte técnicos nos sistemas operacionais Microsoft e Linux com suas sub-denominações, software de backup, antivírus e consultoria em casos de necessidade da intervenção por software de terceiros e gerenciamento, facilitando para que a câmara tenha suporte para que o ambiente de Informática esteja sempre funcional e seguro.
      5. Suporte necessários para auxílio da autarquia nas políticas de licenciamento de software.
      6. Conferência / definições / execução de serviços de realocação dos servidores virtuais;
      7. Suporte e sustentação no ambiente local e virtualizado, firewall, políticas de rede, políticas de backup e recuperação de desastres.
      8. Conferência / Criação / avaliação / reestruturação de usuários e acesso aos recursos de rede e redefinição das políticas de segurança.
      9. Análise/alteração dos servidores de dados e reestruturação para otimização de desempenho.
      10. Levantamento de ativos de rede e licenças (servidores, computadores, impressoras, switchs, roteadores etc.).
      11. Configuração, manutenção e melhores práticas, na rede wifi corporativa composta por Access Points Ubiquiti Unifi juntamente com a controladora física.
      12. Reavaliação das conexões da infraestrutura interna.
      13. Manutenção da conexão.
      14. Redefinição e aplicação de políticas de backups.
      15. Conferência do Backup atual, sendo que o mesmo deve ser configurado de acordo com as premissas e normas, evitando problemas com perda de dados.
      16. Avaliação/definição/aplicação dos serviços de internet e acessos internos e externos dos usuários.
      17. Aplicação e conferência das políticas de firewall (segurança no acesso a Internet).
      18. Visando dar aporte aos usuários, capacitação de profissionais da área de TI, realizar manutenção de toda a rede e dos servidores de dados e consolidar os conceitos e a funcionalidade dos sistemas implantados e/ou readaptados.
      19. Gerar relatórios mensais e/ou Trimestrais referente aos acessos indesejados de acordo com política de Firewall aplicada afim de direcionar os administradores para eventuais bloqueios e medidas para melhoria da qualidade dos serviços prestados pelos servidores.
      20. As manutenções no parque de microcomputadores em sua totalidade deverão ser realizadas pela CONTRATADA, durante a vigência do contrato, independentemente de abertura de chamado técnico, devendo ser organizadas e previamente agendadas.
      21. Por ocasião da manutenção preventiva poderá ser solicitado pela CONTRATANTE, sem custo adicional, a aplicação de patches , servisse packs, fixes e atualizações indicadas pelos fornecedores do sistema operacional e pacotes de aplicativos, levantamento dos dados dos equipamentos instalados e a identificação por meio de etiquetas, sendo o fornecimento das mesmas responsabilidade da CONTRATADA.
      22. Prestação de serviços técnicos de manutenção preventiva e corretiva de “hardware”, manutenção da infraestrutura física e logica da rede de computadores, instalação e apoio a backup, suporte aos usuários no uso do ambiente Windows, MS-Office e outros além de atualizações dos softwares necessários.
      23. Manutenção preventiva e corretiva, impressoras scanners e nobreaks.
      24. As peças de reposição necessárias para o funcionamento dos equipamentos, deverão ter as suas características informadas a CONTRATANTE e, após a devida autorização, poderão ser realizadas as suas substituições.
      25. A CONTRATADA garante que as peças a serem fornecidas para atender aos serviços de manutenção serão novas, e que não são remanufaturas, recondicionadas ou submetidas a quaisquer processos de reutilização de componentes, no todo ou em parte, e com capacidade igual ou superior a que se encontra instalada nos equipamentos.
      26. Todas as peças defeituosas substituídas deverão ser devolvidas a CONTRATANTE
      27. As peças fornecidas deverão ter seus números de série informados no chamado juntamente com o preço de cada uma.
      28. A Nota Fiscal/Fatura das peças utilizadas deverá ser apresentada juntamente na Nota Fiscal/Fatura referente ao custo mensal da prestação de serviço de manutenção no caso de serem compradas pela CONTRATADA.
      29. A CONTRATADA deverá disponibilizar um profissional presencial para acompanhar as demandas e primeiro suporte, este profissional deverá seguir o horário de funcionamento de toda a Câmara Municipal de Itaúna de segunda a sexta de 08:00 as 17:00 incluindo nas reuniões ordinárias da Câmara que ocorrem uma vez por semana .
      30. A assistência técnica aos equipamentos locados em contrato será prestada na modalidade on-site, nos locais de instalação dos equipamentos, sendo todos os equipamentos instalados em Itaúna-MG, a partir da comunicação do (s) defeito (s) pela equipe da CÂMARA MUNICIPAL DE ITAÚNA, via serviço o ou outro meio indicado pela CONTRATADA.
      31. A assistência técnica de garantia, deverá ser fornecida na modalidade de 8x5.
      32. Os chamados técnicos serão categorizados em níveis de severidade e deverão ser atendidos nos prazos definidos, conforme descrito na tabela abaixo:
      33. Deverá ser disponibilizada licença da ferramenta Zoom Meeting, provendo 1 anfitrião e 100 participantes em todo o período do contrato. Justifica-se a indicação da ferramenta já utilizada pela Câmara Municipal de Itaúna. A licença deverá estar em nome da Contratante e todos os custos deverão estar inclusos no item 06 do lote 01.

|  |  |
| --- | --- |
| **DESCRIÇÃO DE NÍVEIS DE SEVERIDADE** | |
| **SLA** | **Descrição** |
| CRÍTICO | Incidente com paralisação do SISTEMA ou SERVIÇOS DE TI, parte importante dele, ou comprometimento gravíssimo de dados, processos ou ambiente. |
| ALTO | Incidente com paralisação de parte do SISTEMA ou SERVIÇOS DE TI, ou comprometimento grave de dados, processos ou ambiente. |
| MÉDIO | Incidente sem paralisação do SISTEMA ou SERVIÇOS DE TI, porém com comprometimento de dados, processos ou ambiente. |
| BAIXO | Incidente sem paralisação do SISTEMA ou SERVIÇOS DE TI e pequeno ou nenhum comprometimento de dados, processos ou ambiente. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | **Incidente** | | | **Requisição** | | |
| **PRIORIDADE** | **SLA DE  ATENDIMENTO** | **CONTATO** | **ATENDIMENTO** | **SOLUÇÃO** | **CONTATO** | **ATENDIMENTO** | **SOLUÇÃO** |
| Muito alta | SLA CRÍTICO | 30 min | 2 horas | 4 horas | 30 min | 4 horas | 8 horas |
| Alta | SLA ALTO | 30 min | 4 horas | 8 horas | 30 min | 8 horas | 16 horas |
| Médio | SLA MÉDIO | 30 min | 6 horas | 12 horas | 30 min | 16 horas | 24 horas |
| Baixo | SLA BAIXO | 30 min | 8 horas | 16 horas | 30 min | 24 horas | 32 horas |

* + 1. O nível de severidade dos chamados deverá ser comunicado à CONTRATADA, no momento de sua abertura.
    2. O atendimento de um chamado técnico será considerado solucionado de acordo com a tabela abaixo:
    3. O nível de severidade de um chamado poderá ser reclassificado pela câmara municipal de Itaúna. Neste caso, haverá nova contagem de prazo, conforme o novo nível de severidade.
    4. Ao final de cada processo de chamado técnico de acionamento do suporte, deverá ser apresentado relatório contendo a data e hora do chamado, do início e do término do atendimento, bem como a identificação do defeito e as providências adotadas, com o devido ateste de servidor designado pela Câmara de Itaúna.
    5. No impedimento da CONTRATADA na resolução do(s) problema(s) quando do chamado técnico, a CONTRATADA deverá disponibilizar equipamento equivalente ou de superior configuração como backup, até que seja sanado o defeito do equipamento da Câmara de Itaúna.
    6. Caso haja 03 (três) chamadas para problemas da mesma natureza, no mesmo equipamento, em um período de 30 (trinta) dias, a CONTRATADA deverá substituir o equipamento por um novo de igual configuração ou superior.
    7. O único caso em que não haverá cobertura da garantia, será para a falha no equipamento ocorrida por problemas elétricos na rede elétrica do órgão ou atos de vandalismo. A ocorrência de problemas elétricos deverá ser comprovada através de laudo técnico de engenheiro, de forma a comprovar a ocorrência da falha por comportamento inadequado da rede elétrica.
  1. Switch 48 portas POE (Lote 02 | Item 01)
     1. CARACTERÍSTICAS GERAIS
        1. Deve ser instalável em rack padrão de 19”, sendo que deverão ser fornecidos os respectivos kit’s de fixação;
        2. Switch ethernet com pelo menos 48 (quarenta e oito) portas 10/100/1000base-t “auto-sensing” com conectores rj-45;
        3. Deve possuir pelo menos 04 (quatro) portas fixas que permitam a inserção de adaptadores 1/10 gigabit ethernet. Estas portas adicionais não podem ser do tipo “combo” com as portas utp.
        4. O switch deve permitir o uso simultâneo de pelo menos 48 portas 1 gigabit ethernet (rj-45), 4 portas 10 gigabit ethernet;
        5. As portas sfp/sfp+ deverão suportar adaptadores para nos padrões:
        6. 10gbase-sr,10gbase-lr e dac (direct attached cable);
        7. 1000-sx e 1000-lx;
        8. O switch fornecido deve suportar as normas técnicas ieee802.3 (10baset), ieee802.3u (100base-tx), ieee 802.3z (1000base-x), ieee 802.3ab (1000base-t);
        9. Deve possuir leds, por porta, que indiquem a integridade e atividade do link;
        10. Possuir fontes de alimentação redundantes internas ao equipamento com ajuste automático de tensão 110 ou 220 volts e 52 volts
        11. Ser fornecido com configuração de cpu e memória (ram e flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação;
        12. O switch deve ter matriz de comutação de pelo menos 176 gbps;
        13. A tela sensível ao toque mínima de 1,3" exibe o status informações para monitoramento fácil e rápido solução de problemas.
        14. Todas as licenças necessárias para as funcionalidades exigidas neste edital deverão estar inclusas no equipamento;
     2. STACKING
        1. O switch fornecido (caso não utilize apenas 1 switch por andar) deve ter nativamente a funcionalidade de stacking/empilhamento.
        2. A funcionalidade de empilhamento deve possuir pelo menos as seguintes características:
        3. A pilha de switches deverá ser gerenciada como uma entidade única;
        4. O empilhamento deve ser feito em anel para garantir que, na eventual falha de um link, a pilha continue a funcionar;
        5. Em caso de falha do switch controlador da pilha, um controlador “backup” deve ser selecionado de forma automática, sem que seja necessária intervenção manual;
        6. Deve ser fornecido um cabo para stack de no mínimo 1,00 metros.
     3. FUNCIONALIDADES GERAIS
        1. Deve ser gerenciável via console central;
        2. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada;
        3. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em um switch remoto no mesmo domínio l2;
        4. Deve possuir suporte a protocolo de autenticação para controle do acesso administrativo ao equipamento;
        5. Deve implementar listas de controle de acesso (acls) baseadas em endereço ip de origem e destino (ipv4 e ipv6), portas tcp e udp de origem e destino e endereços mac de origem e destino;
        6. Deve possuir mecanismos de controle de broadcast, multicast e unicast por porta;
        7. Deve permitir pelo menos uma fila de saída com prioridade estrita por porta e divisão ponderada de banda entre as demais filas de saída;
        8. Além dos protocolos de comutação da camada 2 e recursos, o recursos de camada 3, como roteamento entre VLANs, roteamento estático e Funcionalidade de servidor DHCP.
     4. POE
        1. Potência Mínima 600w
        2. Interface POE
           1. Portas de 1 a 40

POE+ IEEE802.3af/at

* + - * 1. Portas de 41 a 48 802.3af/at, 802.3bt

60w POE++ IEEE 802.3af/at/bt

* + - 1. Watts máxima POE por porta
         1. 802.3at 32W
         2. 802.3bt 64W
      2. Voltagem máxima
         1. 802.3at 44-57V
         2. 802.3bt 50-57V
  1. Office Home and Business (Lote 02 | Item 02)
     1. Compra única para 1 PC com Windows ou Mac
     2. Licença: Vitalícia PC; Mac OS para Mac
     3. Pacote de aplicativos Microsoft Office Home & Business ESD
     4. Linguagem: Português (podendo ser alterado pelo usuário).
     5. Tecnologia: 32 / 64 bits
     6. Suporte técnico nos primeiros 60 dias
     7. Conjunto inclui: Excel; PowerPoint; Word; OneNote; Outlook; Teams Gratuito\*
     8. Confira as aplicações disponíveis no Teams Gratuito:
        1. Chamadas de vídeo e áudio online
        2. Agenda de reuniões
        3. 2 GB de memória
     9. Garantia:
        1. 10 anos de garantia (117 meses de garantia contratual junto ao fabricante + 3 meses referentes à garantia legal, nos termos do artigo 26, II, do Código de Defesa do Consumidor)
  2. Nobreak 1500 VA (Lote 02 | Item 03)
     1. Especificações:
        1. Entrada: Bivolt Automático
        2. Saída: 115V
        3. Nobreak interativo com regulação on-line
        4. Forma de onda senoidal por aproximação (retangular PWM)
        5. Estabilizador interno com 4 estágios de regulação
        6. Filtro de linha interno
        7. Porta fusível externo com unidade reserva
        8. Tomadas de saída NBR 14136: 5 no modelo 1500VA
        9. Extension Cord Grátis: extensão com mais 4 tomadas (nos modelos 1500VA).
        10. Conector de engate rápido: para expansão de autonomia
        11. Autodiagnóstico de bateria: informa o momento certo de trocar a bateria
        12. Battery Saver: prolonga a vida útil da bateria
        13. Microprocessado: Microprocessador RISC de alta velocidade com memória Flash, integrando diversas funções periféricas, aumentando a confiabilidade e o desempenho do circuito eletrônico.
        14. Função TRUE RMS: analisa corretamente os distúrbios da rede elétrica permitindo a atuação precisa do equipamento.
        15. Autoteste: ao ser ligado, o nobreak testa todos os circuitos internos e a presença de aterramento.
        16. Recarregador Strong Charger: Permite a recarga das baterias mesmo com níveis muito baixos de carga, inclusive com o nobreak desligado.
        17. Permite ser ligado na ausência de rede elétrica (DC Start)
        18. Circuito desmagnetizador: garante o valor de tensão adequado na saída do nobreak para equipamentos de informática e similares (cargas não lineares)
        19. Alarme audiovisual para queda de rede, subtensão, fim do tempo de autonomia, final de vida útil da bateria, sobretensão, potência excedida e sobre temperatura
        20. Botão liga/desliga temporizado com função mute
        21. Inversor sincronizado com a rede elétrica (sistema PLL)
     2. Proteções:
        1. Queda de rede (Blackout): Mantém o fornecimento de energia nas saídas durante a ausência total da rede elétrica
        2. Ruído de rede elétrica: Possui filtro de linha interno que atenua ruídos provenientes da rede elétrica, fornecendo energia limpa para os equipamentos
        3. Sobretensão de rede elétrica: Durante a ocorrência deste evento, o UPS utiliza energia das baterias, mantendo a saída em um valor adequado
        4. Subtensão de rede elétrica: Durante a ocorrência deste evento, o UPS utiliza energia das baterias, mantendo a saída em um valor adequado
        5. Surtos de tensão na rede: A rede elétrica pode apresentar picos de tensão provenientes, principalmente por descargas elétricas. A proteção é de modo comum e diferencial (entre fase-neutro ou fase-fase)
        6. Correção de variação da rede elétrica por degrau: A correção da tensão de saída é realizada através do estabilizador interno e é feita por taps de regulação

1. **DO LOCAL DE ENTREGA**
   1. A entrega dos materiais deverá ser realizada na Av. Getúlio Vargas, nº 800, Centro, Itaúna, Minas Gerais, devendo ser previamente agendada utilizando como forma de comunicação oficial o e-mail:[compras@cmitauna.mg.gov.br](mailto:compras@cmitauna.mg.gov.br) e/ou telefone (37) 3249-2066.
   2. Os materiais deverão ser entregues de segunda a sexta-feira dentro do horário de 8h às 16h.
2. **RECEBIMENTO DOS MATERIAIS/SERVIÇOS**
   1. O material será recebido, temporariamente, de uma só vez, na sede da Câmara Municipal de Itaúna/MG, pelo setor de almoxarifado.
   2. O prazo para a entrega do material será de até 15 (quinze) dias contados a partir da publicação oficial do resultado do certame.
   3. Caso os materiais apresentem defeitos ou não sejam compatíveis com as especificações deste anexo e das propostas, a licitante vencedora deverá proceder a substituição no prazo máximo de 05 (cinco) dias úteis.
   4. O material deverá ser entregue em embalagens originais do fabricante, devidamente lacradas.
   5. A aceitação do objeto desta licitação somente será efetivada após o produto ter sido examinado e considerado em condições de uso, quando será declarado o recebimento definitivo.
3. **DAS OBRIGAÇÕES E RESPONSABILIDADES DO FORNECEDOR**
   1. O FORNECEDOR, além do fornecimento dos produtos, obriga-se a:
      1. Fornecer dentro do prazo mencionado o produto licitado e nos horários estabelecidos pela CÂMARA;

6.1.2 Em relação ao faturamento só se efetivará após a conclusão da instalação.

6.1..3 Responsabilizar-se integralmente pela qualidade do serviço realizado.

6.1.4. Comunicar ao fiscal do contrato qualquer empecilho à execução do contratado a tempo de serem tomadas as medidas cabíveis, a fim de que não haja atraso em sua execução.

6.1.5. É expressamente vedada a cessão, subcontratação ou sub-rogação total ou parcial a terceiros para a execução do objeto licitado.

6.1.6. Fornecer o item/serviço licitado com qualidade e segundo especificado no termo de referência.

6.1.7. Manter durante a execução do contrato em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, com apresentação da regularidade com o INSS, FGTS e Trabalhista, por ocasião da entrega das faturas/notas fiscais.

6.1.8. Arcar com as despesas decorrentes de qualquer infração cometida por seus empregados quando do fornecimento do objeto contratado.

6.1.9. Responsabilizar-se por todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução deste contrato, originariamente ou vinculada por prevenção, conexão ou continência.

6.1.10. Responsabilizar-se por todos os encargos fiscais, comerciais, ambientais, trabalhistas e outros resultantes desta contratação.

6.1.11. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados, no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências da CONTRATANTE.

6.1.12. Prestar serviço 24 h por dia, 7 dias por semana, durante todo o período de vigência do contrato.

6.1.13. A CONTRATADA não poderá subcontratar para a execução do objeto deste contrato, sem autorização expressa da CONTRATANTE.

6.1.14. A CONTRATADA deverá empregar os métodos mais modernos pertinentes à execução do serviço, de acordo com as recomendações técnicas, necessários à perfeita execução do serviço, nos prazos.

6.1.15 Responsabilizar-se integralmente pela qualidade dos produtos fornecidos, cumprindo as disposições legais que interfiram em sua comercialização;

1. **DAS OBRIGAÇÕES E RESPONSABILIDADES DO CONTRATANTE**

7.1 Garantir o acesso às informações necessárias para a execução do objeto.

7.2.Atender a todas as condições estabelecidas neste Termo de Referência.

7.3. Notificar ao Fornecedor qualquer irregularidade ou defeito encontrado nos serviços.

7.4. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo Prestador.

7.5.Exercer a fiscalização do serviço contratado.

7.6.Efetuar pagamento em favor da Contratada, até o 5º (quinto) dia após o recebimento definitivo do objeto contratado, através de Ordem Bancária ou cheque, mediante apresentação da respectiva Nota Fiscal/Fatura, devidamente discriminada.

7.7.Rejeitar no todo ou em parte, o serviço em desacordo com as exigências deste Termo de Referência.

**8. DA PROPOSTA COMERCIAL**

A proposta deverá ser confeccionada em papel timbrado do próprio fornecedor, contendo prazo mínimo de 60 (sessenta) dias de validade e deverá ser entregue diretamente na Secretaria Administrativa e Financeira da Câmara Municipal, sediada na Avenida Getúlio Vargas, nº 800, Centro, Itaúna/MG, CEP: 35680-037 ou poderá também ser enviada via e-mail, desde que contenha os dados da empresa, como CNPJ, endereço completo, telefone e e-mail de contato e assinado pelo responsável.