



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

TERMO DE REFERÊNCIA

1. OBJETO:

- 1.1. Registro de preços para eventual contratação de 02 (duas) empresas especializadas na prestação de serviços de telecomunicações através do fornecimento de links de comunicação de dados dedicado à Internet com serviços de proteção contra ataques DDoS, enlaces de dados do tipo Lan to Lan e segurança de dados através de Firewall de nova geração, contemplando a configuração, instalação, gerenciamento proativo e manutenção dos serviços de acordo com as especificações descritas no Termo de Referência, em que o lote 2 visa garantir total redundância para o lote 1, ambos devem ser contratados por operadoras distintas e não poderá ocorrer subcontratação entre as empresas vencedoras dos lotes 1 e 2. Adicionalmente, os caminhos percorridos pelos cabos a serem lançados pela vencedora do Lote 2 deverão percorrer rotas distintas da vencedora do lote 1.

Planilha de Formação de Preços

Lote 1	Link Principal Descrição e Especificações	Quantidade	Valor mensal	Valor total (12 meses)
1	Fornecimento de link de acesso dedicado à Internet na velocidade de 1 Gbps, incluindo gerenciamento proativo e proteção contra ataques do tipo DDoS	1		
2	Fornecimento de enlaces dedicados Lan to Lan na velocidade de 300 Mbps	3		
3	Fornecimento de solução de segurança composto de firewall de nova geração com SD-WAN para a saída de internet	1		
4	Fornecimento de solução de segurança composto de firewall de nova geração com SD-WAN para os enlaces Lan-to-Lan	3		
VALOR TOTAL 12 MESES				

Lote 2	Link Redundante Descrição e Especificações	Quantidade	Valor mensal	Valor total (12 meses)
1	Fornecimento de link de acesso dedicado à Internet na velocidade de 1 Gbps, incluindo gerenciamento proativo e proteção contra ataques do tipo DDoS	1		
2	Fornecimento de enlaces dedicados Lan to Lan na velocidade de 300 Mbps	3		
VALOR TOTAL 12 MESES				



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

2. JUSTIFICATIVA:

A Câmara Municipal do Recife disponibiliza diversos serviços e sistemas para acesso ao público e para o funcionamento dos setores administrativos deste órgão, dentre eles o próprio portal institucional, portal da transparência, serviço de informação ao cidadão - e-sic, SAPL, sistema financeiro entre outros. Além desses, também é disponibilizado o serviço de streaming que realiza a transmissão das reuniões ordinárias, plenarinho ao vivo, audiências públicas e reuniões públicas.

Todos os sistemas e serviços citados anteriormente dependem totalmente de um link de internet para funcionar adequadamente. Sendo assim, faz-se necessária a contratação de empresa para a prestação de serviços de link de internet para esta Câmara. A contratação do link visa garantir o funcionamento adequado desta Casa através do acesso e disponibilidade de informações e de todos os serviços oferecidos para os cidadãos, vereadores e funcionários.

Some-se a isso que, em 2021, a Lei Geral de Proteção de Dados nº 13.709, de 14 de agosto de 2018, entrou em vigência, ampliando as exigências do Marco Civil da Internet e reforçando a utilização de melhores práticas de mercado no que tange aspectos da Segurança da Informação. Tal Lei, a partir de 2021 passa a aplicar sanções administrativas pesadas para entidades privadas e públicas de até R\$ 50.000.000,00 (cinquenta milhões de reais) por infração. A exemplificar, no caso de vazamento de informações de algum banco de dados de usuários desta CONTRATANTE, caracterizaria infração e aplicação de sanção.

Há ainda que se destacar as medidas regulatórias estabelecidas nos últimos anos que necessitam de ferramentas atuais e adequadas para garantir conformidade, como é o caso da LGPD, que conhecidamente, soluções atuais de segurança conseguem contemplar.

O modelo de contratação por meio de compra de produtos e autogestão não é suficiente para atender à nossa necessidade, visto a velocidade com que surgem novos tipos de ameaças e principalmente a velocidade com que o mercado de segurança evolui. Portanto, objetivando a prestação do serviço por profissionais capacitados e especialistas em cibersegurança atuando por meio de um SOC – Security Operations Center, monitoramento do ambiente na modalidade 24x7 (vinte e quatro horas por dia, sete dias por semana), definiu-se pela contratação da solução na modalidade de serviço (as a service).

2.1. Resultados e Benefícios a Serem Alcançados:

Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

Aprimorar a segurança de TIC da Câmara Municipal do Recife frente a ameaças sofisticadas;



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

Possibilitar o controle de acesso e complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;

Possibilitar o acesso remoto de maneira estável aos colaboradores de forma segura;

Prestar os serviços de TIC mantendo a segurança adequada às informações organizacionais, principalmente quanto à garantia de disponibilidade e integridade dos dados necessários ao pleno funcionamento dos processos administrativos;

Assegurar a sustentabilidade e desempenho dos serviços, conforme sua nova topologia e tráfego de rede;

Aumento da capacidade de resposta incidentes de segurança.

3. DEFINIÇÕES:

3.1. Backbone: infraestrutura de interligação de uma rede, constituída de roteadores de borda do provedor e roteadores de núcleo, bem como os circuitos que existam entre eles.

3.2. ANATEL: Agência Nacional de Telecomunicações.

3.3. CPE (de Customer Premises Equipment): é um termo técnico muito utilizado por operadoras de telecomunicações e fornecedores de serviços de comunicação. Se trata do equipamento instalado dentro das instalações do cliente para prestação do serviço pela Operadora.

3.4. DNS: de *Domain Name System*, ou “Sistema de Nomes de Domínios”. Trata-se, de servidores que armazenam listagens de domínios e seus respectivos endereços IPs. são os responsáveis por localizar e traduzir para números IP os endereços dos sites utilizados nos navegadores.

3.5. HTTP: O *Hypertext Transfer Protocol*, é um protocolo de comunicação utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web. Hipertexto é o texto estruturado que utiliza ligações lógicas entre nós contendo texto.

3.6. IP (de Internet Protocol): é um protocolo de comunicação usado para encaminhamento dos dados entre equipamentos em rede, utilizando endereços alocados em cada um dos elementos da mesma (endereços IP).

3.7. Last Mile ou Última Milha: circuito dedicado entre o roteador de borda do provedor e o roteador ou switch existente nas dependências do cliente.

3.8. MTTR: de *Mean Time to Repair* é um indicador de desempenho usado na manutenção para indicar o Tempo Médio Para Reparo de algum equipamento, componente, máquina ou sistema.



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

3.9. Router ou Roteador: equipamento tipicamente utilizado para fazer a interface entre uma rede local e uma rede de telecomunicações. É usado também nos nós de uma rede para processar roteamento do tráfego IP.

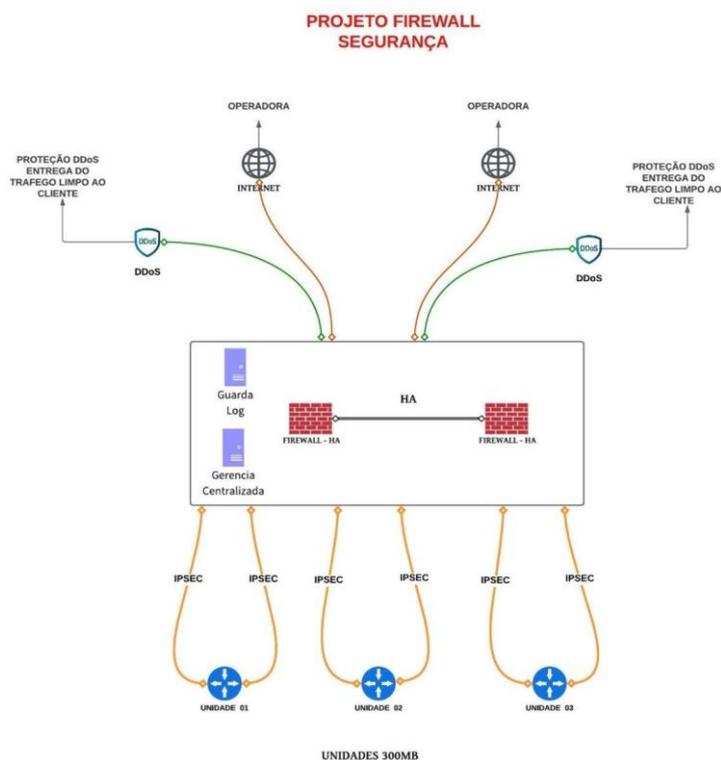
3.10. SLA: Service Level Agreement, que é traduzido em português por ANS (Acordo de Nível de Serviço). Refere-se à especificação, em termos mensuráveis e claros, de todos os serviços que o contratante pode esperar do fornecedor na negociação.

3.11. SNMP (Simple Network Management Protocol): protocolo de gerenciamento usado normalmente em redes IP.

3.12. DDoS (Distributed Denial of Service): é um ataque distribuído, o qual pode estar vinculado à milhares de computadores com interesse malicioso.

3.13. Solução de segurança NGFW: é uma solução projetada para resolver ameaças cibernéticas avançadas no nível do aplicativo por meio de recursos de segurança com reconhecimento de contexto e inteligência, combinando recursos convencionais de firewall, como inspeção de estados (stateful inspeção) e filtragem de pacotes, com outros avançados para tomar decisões sobre que tipo de tráfego permitir. Possui a capacidade de filtrar pacotes com base em aplicativos e inspecionar os dados armazenados nos pacotes (não se limitando a cabeçalhos IP, como os firewalls tradicionais)

4. TOPOLOGIA DA SOLUÇÃO:





CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

5. ESPECIFICAÇÕES TÉCNICAS DOS LINKS:

5.1. REQUISITOS GERAIS

- 5.1.1. Toda a infraestrutura de rede, acesso e CPE da CONTRATADA deverão ser dimensionadas e preparadas para suportar a totalidade do serviço.
- 5.1.2. A CONTRATADA deverá reservar os canais de comunicação e as portas de acesso à sua infraestrutura para uso exclusivo da CONTRATANTE, não sendo admitido o compartilhamento desses recursos com outro de seus clientes ou usuários.
- 5.1.3. O acesso referido no item anterior deverá ser provido por meio de backbone próprio da prestadora de serviço.
- 5.1.4. Os equipamentos da CONTRATADA utilizados em toda a solução deverão ser novos e compatíveis com ambientes corporativos.
- 5.1.5. A CONTRATADA obriga-se e se responsabiliza a prestar o serviço objeto da licitação, por meio de mão de obra especializada e devidamente qualificada, necessária à completa e perfeita execução dos serviços, em conformidade com as especificações do Termo de Referência.
- 5.1.6. Será de responsabilidade da CONTRATANTE o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede elétrica e a climatização das dependências.
- 5.1.7. Uma vez que o lote 2 visa garantir total redundância para o lote 1, ambos devem ser contratados por operadoras distintas e não poderá ocorrer subcontratação entre as empresas vencedoras dos lotes 1 e 2.
- 5.1.8. Os caminhos percorridos pelos cabos a serem lançados pela vencedora do Lote 2 deverão percorrer rotas distintas da vencedora do lote 1.

5.2. CARACTERÍSTICAS DO LINK INTERNET (ITEM 1 DOS LOTES 1 E 2)

- 5.2.1. Fornecer e instalar link de Internet na taxa de 1 Gbps.
- 5.2.2. A CONTRATADA deverá disponibilizar 8 endereços IPV4 e 32 endereços IPV6 fixos e válidos para provimento da solução de Internet.
- 5.2.3. Contratação de empresa especializada para o fornecimento de acesso à Rede Mundial de Internet com 100% de garantia de banda downstream e upstream, full-duplex, com conectividade em protocolos IPv4 e IPv6.
- 5.2.4. A CONTRATADA deverá atender as seguintes exigências de conexões de Backbone IP para estar apta a prestar os serviços de Internet especificados neste Termo de Referência:
 - 5.2.4.1. AS LICITANTES VENCEDORAS devem comprovar, em suas propostas comerciais, possuir uma conexão de no mínimo 10 Gbps com o PTT (Ponto de Troca de Tráfego) Recife ou São Paulo gerido pelo IX.br, podendo esta conexão



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

ocorrer através de qualquer PIX (Ponto de Interconexão) membro;

5.2.4.2. AS LICITANTES VENCEDORAS devem comprovar, em suas propostas comerciais, possuir uma conexão de no mínimo 2 Gbps com o PTT (Ponto de Troca de Tráfego Distrito Federal pelo IX.br, para entregar a melhor experiência de acessos a conteúdos nacionais e governamentais; podendo esta conexão ocorrer através de qualquer PIX (Ponto de Interconexão) membro;

5.2.4.2.1. IX.br é o nome dado ao projeto do Comitê Gestor da Internet no Brasil (CGI.br) que promove e cria a infraestrutura necessária (Ponto de Intercâmbio de Internet - IXP) para a interconexão direta entre as redes ("Autonomous Systems" - ASs) que compõem a Internet Brasileira;

5.2.4.2.2. A CONTRATADA deve garantir que todo o tráfego de Internet que tenha como destino as redes dos membros participantes de qualquer PIX de Recife sejam roteados diretamente para eles através da conexão do serviço de Internet Corporativa (IC) da CONTRATADA com o IX, podendo esta conexão ocorrer através de qualquer PIX, garantindo o menor salto e latência na comunicação;

5.2.4.2.3. A CONTRATADA deve garantir que em caso de falha na comunicação com o IX ou PIX, a conexão com as redes dos participantes continuem disponíveis através de outras rotas de interconexão da CONTRATADA sem causar indisponibilidade

5.2.4.3. AS LICITANTES VENCEDORAS devem comprovar, em suas propostas comerciais, estarem conectadas a pelo menos um PTT Internacional, ou que possuem contratos de trânsito IP com pelo menos duas empresas que estejam conectadas a algum PTT Internacional. Entenda-se por PTT Internacional aquele que se acha fora dos limites da jurisdição territorial da União. A comprovação de que a empresa está conectada a algum PTT Internacional será feita através do site: https://bgp.he.net/ASXYZ#_ix, onde XYZ é o número do AS da empresa licitante.

5.2.4.4. AS LICITANTES VENCEDORAS devem apresentar um documento impresso com as informações da licitante que constam no site <http://bgp.he.net/> - dentre elas: o número do AS da licitante, os peers IPv4 e IPv6 e os pontos de interconexão IX (Internet eXchange) em que a licitante está conectada.

5.2.4.5. AS LICITANTES VENCEDORAS devem comprovar, em suas propostas comerciais, que o somatório das larguras de banda de seus backbones, considerando conexões com Pontos de Troca de Tráfego Nacionais, links dedicados com empresas com backbone Nacional e trânsito IP para PTT internacionais, resultem em um total de no mínimo 60 (Sessenta) Gbps.

5.2.5. A conexão entre o CPE da CONTRATADA e o equipamento da CONTRATANTE deverá



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

ser realizada através de interface Gigabit Ethernet 1000BASE-T.

- 5.2.6.** A CONTRATADA não poderá utilizar acessos de terceiros como última milha.
- 5.2.7.** O acesso físico (conexão entre o ponto de presença da CONTRATADA e os equipamentos de comunicação de dados da CONTRATADA instalados nas dependências da CONTRATANTE) deverá ser realizado exclusivamente por meio de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso.
- 5.2.8.** A CONTRATADA deverá:
- 5.2.8.1.** Instalar o ponto de acesso físico (fibra óptica), a instalação do cabeamento externo e interno (do perímetro da CONTRATANTE), as obras para acomodação de meio físico e quaisquer outras providências que tenham relação direta com a entrega do serviço. A CONTRATANTE será responsável apenas pela disponibilização dos pontos elétricos (220v), aterramento e espaço físico
 - 5.2.8.2.** Instalar e configurar todos os equipamentos (modems, roteadores e cabos) e demais acessórios necessários à operação dos circuitos (fibra óptica), e a manutenção e atualização do sistema operacional de roteadores, sem ônus adicionais para a CONTRATANTE.
 - 5.2.8.3.** O roteador (CPE) não deverá exceder carga máxima de CPU e memória acima de 70%. Caso seja identificado, durante a execução do contrato, utilização acima deste limite, em um intervalo de 5 minutos, este deverá ser substituído, atualizado e/ou configurado, sem ônus adicional para a CONTRATANTE.
 - 5.2.8.4.** A CONTRATADA deverá implementar e garantir o acesso de consulta (via SNMP v3) a CPE instalada no PP, para permitir o monitoramento do tráfego.
 - 5.2.8.5.** Instalar o serviço de Internet Corporativa de forma a concentrar o roteamento de todo o fluxo de tráfego da rede, obrigando que todos os pacotes das unidades remotas com destino à Internet passem neste ponto. Prover equipamentos com capacidade adequada para garantir o desempenho necessário para rotear todo tráfego Internet que estará conectados em suas interfaces.
 - 5.2.8.6.** Implementar o aumento ou redução da velocidade, quando solicitado, de forma transparente. As atualizações tecnológicas requisitadas para este aumento ou redução de velocidade devem ser suportadas pelos recursos e equipamentos envolvidos na solução. A velocidade indicada ao atendimento do Serviço Internet, não poderá, a qualquer tempo, ser formada pela composição (somatório) de acessos com taxas inferiores à solicitada. A CONTRATADA deverá comunicar a CONTRATANTE da necessidade do aumento da velocidade, quando o uso da banda atingir picos de consumo, em horário de maior movimento (HMM), de 80% da capacidade contratada, através de documento com análise se medições previamente elaboradas, e será executada mediante Parecer Técnico e Ordem de Serviço específica emitida pela CONTRATANTE.
 - 5.2.8.7.** Prover serviços Internet para todas as unidades da CONTRATANTE conectadas a através do PP, compartilhando e provendo serviços aos usuários desta rede.



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 5.2.8.8.** Realizar o gerenciamento do Acesso à Internet a partir do PP, provendo equipamentos, softwares e Roteadores com capacidade adequada para garantir o desempenho necessário para rotear todo tráfego Internet que estará conectado em suas interfaces.
- 5.2.8.9.** Disponibilizar uma solução de sistema de gerência para o serviço de Internet de forma integrada, visando o controle e monitoramento de seus recursos e capacidades, provendo informações detalhadas e gerenciais para a CONTRATANTE referente aos Níveis de Qualidade efetivamente realizados para assegurar a realização dos atestos e pagamentos dos serviços efetivamente entregues e operacionalizados.
- 5.2.8.10.** Permitir o acesso somente leitura da CONTRATANTE ao roteador de acesso a fim de possibilitar o monitoramento dos serviços. O acesso deverá ser permanente, dedicado e exclusivo à Internet Mundial com total conectividade IP.
- 5.2.8.11.** Adotar o protocolo TCP/IP na modalidade dedicada conectada à Internet Mundial, incluindo toda a infraestrutura de equipamentos, meios de acesso e serviços necessários para este fim.
- 5.2.8.12.** Possuir e oferecer acesso à Internet com canais dedicados e exclusivos interligado diretamente ao backbone próprio da Contratada, comprovando ter seu próprio Endereçamento IP (Autonomous System) sem utilizar meios de transporte por outra empresa intermediária;

- 5.2.9.** O serviço de Internet deverá ser entregue em rede roteada, utilizando protocolos de camada 3, com SLA 99,5% de disponibilidade e MTTR de 4 horas.
- 5.2.10.** Disponibilizar serviço de Domain Name Resolution (DNS) da CONTRATADA, capaz de resolver direta e reversamente endereços de Internet, para registro no servidor DNS primário.
- 5.2.11.** Ser monitorado em regime 24x7 por centro de monitoração da CONTRATADA, sendo responsável pela administração e gerência de equipamentos e links de comunicação de dados, manutenção dos níveis mínimos de serviços exigidos e prevenção e recuperação de falhas de serviço.
- 5.2.12.** A CONTRATADA não poderá:
 - a) Implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego originado ou destinado à CONTRATANTE, a menos que tenha expressa concordância com esta.
 - b) Implementar nenhum tipo de cache transparente, a menos que tenha expressa concordância da CONTRATANTE.
 - c) Realizar a prática de traffic shapping no CPE a ser instalado para a internet

- 5.3. CARACTERÍSTICAS DO ROTEADOR DO LINK DE INTERNET (ITEM 1 DOS LOTES 1 E 2)**



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

5.3.1. O roteador a ser instalado no ambiente da CONTRATANTE deverá ter no mínimo as seguintes características técnicas:

- a) O equipamento e seus módulos e softwares não deverão constar em nenhuma lista do fabricante com as situações de “End-of-Sale”, “End-of-Order”, “End-of-Life” ou “End-of-Support”.
- b) Deve possuir no mínimo 4 interfaces Gigabit Ethernet padrão 1000BASE-T.
- c) Possuir protocolo SNMP habilitado com acesso de leitura.
- d) Deve implementar os protocolos de roteamento RIP, OSPFv2, OSPFv3 e BGP-4.
- e) Deve possuir suporte nativo ao protocolo IPv6.
- f) Deve possuir suporte ao protocolo Netflow v9 ou superior.
- g) Deve possuir suporte ao protocolo 802.1q.
- h) Deve possuir suporte aos protocolos Telnet e SSHv2.
- i) Deve possuir gerenciamento local através de uma porta console, sendo que todos os cabos e adaptadores necessários para o gerenciamento através da porta console deverão ser fornecidos pela CONTRATADA de forma a propiciar o gerenciamento do roteador a partir de uma porta USB.
- j) Deverá ser disponibilizado para a CONTRATANTE com o último release de software estável disponibilizado pelo fabricante, capaz de atender a todos os requisitos acima, incluindo o suporte à atualização do referido software durante o período de vigência do contrato.
- k) Deve ser montável em rack padrão EIA-310 com largura padrão 19” ocupando no máximo 1U de altura.

5.4. CARACTERÍSTICAS DO SERVIÇO Anti DDoS (PROTEÇÃO CONTRA ATAQUES VOLUMÉTRICOS AO LINK DE INTERNET) (ITEM 1 DOS LOTES 1 E 2)

- 5.4.1.** Para proteção da Internet, a CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviço, evitando assim a saturação da banda contratada e a indisponibilidade dos serviços em momentos de ataques DOS (Denial of Service) e DDOS (Distributed Denial of Service);
- 5.4.2.** O serviço de Internet deverá ser fornecido através de Autonomous System Number (ASN) da CONTRATADA, ambiente o qual deverá ocorrer a mitigação dos ataques DOS e DDOS;
- 5.4.3.** A técnica ANTI-DDOS utilizada deverá ser por métrica de volumetria, assim a CONTRATADA deverá enviar junto com a proposta técnica, qual a topologia utilizada para mitigação de ataques DDOS sobre o circuito de dados fornecido;
- 5.4.4.** A CONTRATADA terá no máximo 15 minutos para iniciar a mitigação de ataques de DOS e DDOS;
- 5.4.5.** Não haverá taxa adicional por volume de mitigação de ataques (DDoS – Distributed Denial of Service) nos IPs monitorados;



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 5.4.6.** O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços providos pela CONTRATANTE através da Internet Corporativa (IC) continuem disponíveis;
- 5.4.7.** A limpeza do tráfego deverá ser seletiva e atuar somente sobre os pacotes destinados ao IP atacado, todo tráfego restante não deverá sofrer nenhuma forma de limpeza;
- 5.4.8.** A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos;
- 5.4.9.** A CONTRATADA deve tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDOS, recuperando o pleno funcionamento do mesmo;
- 5.4.10.** Nos períodos de ataque a latência do circuito deverá ser de no máximo 75ms (setenta e cinco milissegundos), sendo permitida a mitigação em centros de limpeza fora do território brasileiro;
- 5.4.11.** A análise realizada para fins da solução deverá ser passiva sem utilização de elementos da rede da CONTRATANTE para coleta dos dados a serem analisados;
- 5.4.12.** A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;
- 5.4.13.** Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da CONTRATADA;
- 5.4.14.** Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS da CONTRATADA, devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo;
- 5.4.15.** Realizar a comunicação da ocorrência do ataque à CONTRATANTE em até 24 horas após a detecção;
- 5.4.16.** Ser capaz de detectar um ataque DDoS automaticamente, ou manualmente, e realizar mitigação na nuvem para apenas o tráfego atacado, contudo na infraestrutura da CONTRATADA, e só redirecionar o tráfego para a REDE da CONTRATANTE quando este estiver limpo deste tipo de ataque;
- 5.4.17.** Realizar a sinalização entre a REDE da CONTRATANTE e a rede da CONTRATADA em qualquer protocolo protegido, podendo ser ativada por qualquer uma das contramedidas especificadas neste serviço;
- 5.4.18.** Após a identificação do ataque por volumetria e direcionamento do tráfego para o centro de limpeza, todas as funcionalidades abaixo devem ser realizadas:
 - 5.4.18.1.** Suportar mitigação de ataques que visam vulnerabilidades nas Camadas 3 OSI, 4 OSI e 7 OSI;
 - 5.4.18.2.** Prover informações de origem de ataque dos países, intervalos (ranges) de endereços IP e características do tipo de ataque;



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife – PE

- 5.4.18.3.** Prover serviço de atualização de assinaturas de ataques das soluções de detecção e mitigação;
- 5.4.18.4.** Ser capaz de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo, mas não se restringindo aos seguintes: Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;
- 5.4.18.5.** Ataques à pilha TCP, incluindo mal-uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;
- 5.4.18.6.** Realizar autenticação de conexão TCP, quando do recebimento de pacotes syn; lecionar se bloqueia apenas o ataque ou o host temporariamente;
- 5.4.18.7.** Possuir autenticação em query DNS por requisição em TCP;
- 5.4.18.8.** Possuir autenticação em JavaScript e Redirect para HTTP;
- 5.4.18.9.** Adicionar expressão regular de “payload” em blacklists;
- 5.4.18.10.** Limitar o número de conexões TCP simultâneas de um mesmo host;
- 5.4.18.11.** Ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
- 5.4.18.12.** Ataques de Botnets e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);
- 5.4.18.13.** DNS BlackList;
- 5.4.18.14.** RegEx para registros específicos ou “flags de recursão”;
- 5.4.18.15.** Possuir mecanismos que permita bloquear um ataque por expressão regular DNS;
- 5.4.18.16.** Prevenir que hosts válidos sejam adicionados a blacklists por engano;
- 5.4.18.17.** Manter lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro;
- 5.4.18.18.** Possuir serviço de atualização de assinaturas de ataques para as soluções de ação e mitigação;
- 5.4.18.19.** Prover a mitigação de ataques baseada em arquitetura na qual haja o desvio de tráfego suspeito, comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;
- 5.4.19.** Possuir no mínimo um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento por meio de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;
- 5.4.20.** Possuir ao menos um centro de limpeza nacional com capacidade de mitigação de 40 Gbps e pelo menos mais 15 (quinze) centros de limpeza internacional com capacidade de mitigação de pelo menos 100 Gbps;



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 5.4.21.** Evitar saturação da banda de Internet em caso de ataques distribuídos de negação de serviço (Distributed Denial of Service - DDoS) com capacidade de mitigação de pelo menos 40 Gbps;
- 5.4.22.** As funcionalidades de monitoramento, detecção e mitigação de ataques são mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;
- 5.4.23.** A mitigação de ataques DDoS é iniciada em até 15 minutos da emissão do alerta;
- 5.4.24.** Deve disponibilizar um portal com dashboard onde a CONTRATANTE tenha acesso online aos tipos de ataques sofridos e o tamanho destes ataques categorizados por severidade (Ex.: Baixo, Médio, Alto), considerando informações atualizadas no portal em até 24 horas após o ataque;
- 5.4.25.** A CONTRATADA deverá fornecer/apresentar relatório analítico enviado mensalmente para a CONTRATANTE;
- 5.4.26.** Em momentos de ataques DoS e DDoS, todo tráfego limpo deve ser reinjetado na infraestrutura da contratante através de conexões diretas entre a plataforma de DoS e DDoS da CONTRATADA e o ambiente do CONTRATANTE e/ou utilização da técnica VRF (Virtual Routing and Forwarding) via BGP Full.

5.5. CARACTERÍSTICAS DOS ENLACES LAN TO LAN (ITEM 2 DOS LOTES 1 E 2)

- 5.5.1.** A Conexão do enlace deverá ser do tipo ponto a ponto utilizando tecnologia de rede Metro Ethernet e serão instalados para permitir a conexão das unidades remotas da CONTRATANTE com o PP, formando uma rede de alta velocidade, garantindo a bandasimétrica contratada.
- 5.5.2.** Fornecer, instalar e configurar 3 (três) enlaces Lan to Lan na velocidade de 300 Mbps conforme endereços especificados neste Termo de Referência.
- 5.5.3.** A conexão entre o CPE da CONTRATADA e os equipamentos de segurança/SD-WAN, previstos nos itens 3 e 4 do lote 1, deverá ser realizada através de interface Gigabit Ethernet 100BASE-T.
- 5.5.4.** A CONTRATADA não poderá utilizar acessos de terceiros como última milha
- 5.5.5.** O acesso físico (conexão entre o ponto de presença da CONTRATADA e os equipamentos de comunicação de dados da CONTRATADA instalados nas dependências da CONTRATANTE) deverá ser realizado exclusivamente por meio de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso.
- 5.5.6.** O serviço de Internet deverá ser entregue em rede roteada, utilizando protocolos de camada 3, com SLA 99,5% de disponibilidade e MTTR de 4 horas.
- 5.5.7.** Ser monitorado em regime 24x7 por centro de monitoração da CONTRATADA, sendo responsável pela administração e gerência de equipamentos e links de comunicação de dados, manutenção dos níveis mínimos de serviços exigidos e prevenção e recuperação de falhas de serviço.



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 5.5.8.** Disponibilizar informações sobre os serviços de acesso à internet por meio de um portal de monitoramento, com acesso restrito, utilizando protocolo seguro (HTTPS), contendo estatísticas de desempenho e de disponibilidade do acesso.
- 5.5.9.** Possibilitar que a equipe técnica da CONTRATANTE realize consultas no portal de monitoramento, bem como visualize relatórios das informações de desempenho dos serviços contratados.
- 5.5.10.** A CONTRATADA deverá:
- 5.5.10.1.** Instalar, operacionalizar e manter os serviços. Para cada link devem ser disponibilizados, de forma integrada e gerenciável, os serviços de dados, voz e imagens, suportados pelo protocolo TCP/IP. Conforme já requerido nas subseções acima, reitera-se que este serviço inclui todos os recursos de conectividade e as atividades de configurações de todos os recursos envolvidos imprescindíveis, modems, roteadores e switches, assim como o cabeamento, as calhas e os racks que se fizerem imprescindíveis para o seu pleno funcionamento
 - 5.5.10.2.** Garantir o sigilo e a integridade dos dados e imagens transmitidos através dos links.
 - 5.5.10.3.** Permitir gerenciar os serviços em conjunto com a Equipe de Gestão da CONTRATANTE e a equipe de gerência da Contratada para esta finalidade, devendo fornecer os acessos das soluções adotadas, incluindo as informações necessárias para realizar o monitoramento dos níveis de qualidade de forma poder exercer as atividades supervisão e gestão técnica dos Níveis de Serviços neste Termo de Referência.
 - 5.5.10.4.** Garantir que todos os links sejam gerenciados através do protocolo SNMP. O sistema de gerência deve ser integrado, para o controle e monitoramento dos recursos e serviços.

6. DA SOLUÇÃO DE SEGURANÇA NGFW (ITENS 3 E 4 DO LOTE 1)

6.1. Além dos links de comunicação de dados aqui descritos, a contratada do lote 1 deverá fornecer também uma solução de segurança e SD/WAN composta de:

- 6.1.1.** Uma solução, a ser implantada na sede da Câmara do Recife, composta de firewall de nova geração juntamente com ferramentas de gestão e armazenamento de logs, responsável por congrega e garantir a segurança dos dados transmitidos nos os links de saída para a internet e dos lan-to-lan, principais e secundários, aqui denominado de PP.
- 6.1.2.** Uma solução, a ser implantada em cada um dos endereços destino dos Lan-to-lan, composta de firewall de nova geração com função SD-WAN, aqui denominados remotos.

6.2. CARACTERÍSTICAS DA SOLUÇÃO DO PP (ITEM 3 DO LOTE 1)



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 6.2.1.** Solução de Firewall de nova geração, a ser instalada em HA
- 6.2.1.1.** Firewall Throughput de, no mínimo, 11 Gbps, com tamanho do pacote UDP 64byte;
 - 6.2.1.2.** Suporte a, no mínimo, 3 milhões conexões simultâneas;
 - 6.2.1.3.** Suporte a, no mínimo, 275 mil novas conexões por segundo;
 - 6.2.1.4.** Throughput de, no mínimo, 12 Gbps de VPN IPSec com pacotes de 512 bytes;
 - 6.2.1.5.** Estar licenciado para, ou suportar sem o uso de licença, 16.000 mil túneis de VPN IPSEC Site-to-Site simultâneos;
 - 6.2.1.6.** Suportar no mínimo 4 Gbps de throughput de Inspeção SSL;
 - 6.2.1.7.** Deve possuir, pelo menos: 16 interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade;
 - 6.2.1.8.** Deve possuir, pelo menos 8 portas SFP 1 Gigabit Ethernet
 - 6.2.1.9.** Deve possuir 1 porta console
 - 6.2.1.10.** Deve possuir no mínimo 4 interfaces de 10 Gigabit Ethernet
 - 6.2.1.11.** Deve possuir no mínimo 1 porta USB. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet e poder colocar nas zonas de SD-WAN;
 - 6.2.1.12.** Deve possuir fonte redundante;
 - 6.2.1.13.** Estar licenciado, sem custo adicional, para no mínimo 4 sistemas de instancias virtuais (Contextos) por equipamento;
 - 6.2.1.14.** Os equipamentos fornecidos para a solução de Rede e Firewall devem ter uma arquitetura específica e dedicada (appliance), não podendo utilizar equipamentos do tipo servidor de uso genérico, e o sistema operacional deve estar integrado na mesma solução, ou seja, hardware e software devem ser integrados em um único equipamento;
 - 6.2.1.15.** A solução, deverá ser implementada por meio de 2 (dois) equipamentos Appliance Next Generation Firewall (NGFW) idênticos, novos e primeiro uso.
 - 6.2.1.16.** Os equipamentos fornecidos para o serviço de segurança de rede e firewall devem funcionar em alta disponibilidade (HA High Availability) devendo operar no modo ativo/ativo ou ativo/passivo .
- 6.2.2.** Requisitos para solução de gerenciamento centralizado, para configuração do firewall CPE e geração de relatórios, incluindo garantia junto ao fabricante, para atualização de versões, patches e bugs, incluindo suporte técnico 24x7:
- 6.2.2.1.** A CONTRATADA deverá prover um software de gerenciamento com as seguintes informações de cada link dos equipamentos CPE de Segurança da rede;
 - a) Taxa de transmissão e recepção de dados;
 - b) Quantidade de sessões ativas;
 - c) Jitter;
 - d) Latência;
 - e) Perda de Pacotes;



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 6.2.2.2.** O software de gerenciamento deve ser capaz de propagar configurações e atualização de Firmware para todos os equipamentos CPE de Segurança fornecidos e instalados pela CONTRATADA;
- 6.2.2.3.** O software de Gerenciamento do CPE de Segurança pode ser disponibilizado em nuvem ou instalado localmente no Data Center da CONTRATANTE (Máquina Virtual ou Appliance Físico);
- 6.2.2.4.** A equipe técnica da CONTRATANTE deverá ter acesso ao software de gerenciamento do CPE de Segurança;
- 6.2.2.5.** A CONTRATADA deverá fornecer as licenças do software de gerenciamento incluindo garantia junto ao fabricante, para atualização de versões, patches e bugs, incluindo suporte técnico 24x7;
- 6.2.2.6.** Garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
- 6.2.2.7.** Definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 6.2.2.8.** Gerar alertas automáticos via e-mail e SNMP para destinatários definidos pela equipe responsável do CONTRATANTE;
- 6.2.2.9.** Possibilitar a criação e administração de políticas de firewall, controle de aplicação, Sistema prevenção à intrusão (IPS – Intrusion Prevention System), Antivírus, pontos de acesso sem fio e de Filtro de URL;
- 6.2.2.10.** Permitir usar palavras chaves ou cores para facilitar identificação de regras;
- 6.2.2.11.** Permitir localizar quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;
- 6.2.2.12.** Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;
- 6.2.2.13.** Permitir criação de regras que fiquem ativas em horário definido;
- 6.2.2.14.** Permitir criação de regras com data de expiração;
- 6.2.2.15.** Realizar o backup das configurações para permitir o retorno (rollback) de uma configuração salva;
- 6.2.2.16.** Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso;
- 6.2.2.17.** Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas
- 6.2.2.18.** Garantir que todos os CPEs de Segurança sejam controlados de forma centralizada, utilizando apenas uma plataforma de gerência;
- 6.2.2.19.** Garantir que os CPEs de Segurança sejam visualizados através de geolocalização, e integrados com uma aplicação de mapas online (Google Maps, Bing Maps ou outra equivalente);



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 6.2.2.20.** Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
 - 6.2.2.21.** Permitir ao administrador transferir os backups para um servidor SFTP;
 - 6.2.2.22.** Garantir que as alterações realizadas em um servidor de gerência sejam automaticamente replicadas para o servidor redundante;
 - 6.2.2.23.** A plataforma de gerenciamento deve ser exclusiva para as funções de gerência, ou seja, não deve exercer outras funcionalidades, como exemplo, as de firewall
 - 6.2.2.24.** Continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos gerenciados com o serviço de gerência;
 - 6.2.2.25.** Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota, de maneira centralizada;
 - 6.2.2.26.** Permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS, de bases externas LDAP e RADIUS, de acordo com o modelo de autenticação adotado sendo definido pela CONTRATANTE;
- 6.2.3.** A solução de Guarda de Logs e Relatoria deve possuir as seguintes capacidades e características:
- 6.2.3.1.** Deve possuir capacidade de receber ao menos 25 Giga Bytes de logs diários;
 - 6.2.3.2.** Deve possuir taxa sustentada de 20 mil logs por segundo;
 - 6.2.3.3.** Permitir a criação de painéis (dashboards) customizados para visibilidade do tráfego de aplicações, categorias de URL, ameaças, serviços, países, origem e destino;
 - 6.2.3.4.** Garantir a capacidade de criar consultas SQL ou semelhante para uso nos gráficos e tabelas e relatórios;
 - 6.2.3.5.** Garantir a geração de relatórios com mapas geográficos, ou modo tabela, gerados em tempo real, para visualização de origens e destinos de tráfego;
 - 6.2.3.6.** Permitir a geração de relatório de logs de tráfego dedados;
 - 6.2.3.7.** A solução deve prover exportação de dados via CSV;
 - 6.2.3.8.** Permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos;
 - 6.2.3.9.** Deve ser capaz de receber, armazenar e processar o log de todos os dispositivos de segurança;
 - 6.2.3.10.** A solução Guarda de Logs e Relatoria pode ser fornecida através da técnica de virtualização em equipamentos do tipo Servidor ou através de um provedor de Nuvem.
 - 6.2.3.11.** Garantir uma infraestrutura para receber e consolidar os logs (tipo syslog) de todos os CPE de Segurança da CONTRATANTE por 60 dias com acesso online.



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 6.2.3.12.** Todos os logs devem ser disponibilizados para exportação com acesso apenas de leitura para a CONTRATANTE.
- 6.2.3.13.** Possibilitar a contingência do backup, desde o início da prestação do serviço, na infraestrutura da CONTRATANTE.
- 6.2.3.14.** Possibilitar, de forma centralizada, a visualização dos logs recebidos por um ou vários dispositivos externos, incluindo a capacidade de uso de filtros nas pesquisas deste log;
- 6.2.3.15.** Garantir que a solução atue como um servidor de syslog, aceite e concentre logs de todos os dispositivos de diferentes fabricantes da rede.

6.3. CARACTERÍSTICAS DA SOLUÇÃO DOS PONTOS REMOTOS (ITEM 4 DO LOTE 1)

- 6.3.1.** Para as unidades remotas, com velocidade de 500 Mbps, a CONTRATADA deverá instalar um modelo de equipamento CPE de Segurança, por comodato, capaz de garantir IPsec VPN com Throughput maior ou igual a 500 Mbps e com as seguintes características:
 - 6.3.1.1.** Deve ter capacidade para no mínimo 500 mil sessões simultâneas
 - 6.3.1.2.** Deve ter capacidade para novas sessões de no mínimo de 25 mil por segundo;
 - 6.3.1.3.** Deverá possuir capacidade de encaminhamento de pacotes de 4 Gbps;
 - 6.3.1.4.** Deve possuir throughput de pelo menos 160 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: Controle de Aplicação, IPS, Antivírus, Antispyware e Anti-malware;
 - 6.3.1.5.** Deverá possuir capacidade de inspeção de túneis SSL de 160 Mbps;
 - 6.3.1.6.** Deverá possuir a capacidade de dividir administrativamente, bem como alocar recursos específicos para no mínimo, 2 domínios virtuais ou contextos;
 - 6.3.1.7.** Deve possuir 1 porta USB. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet e poder colocar nas zonas de SD-WAN;
 - 6.3.1.8.** Suportar no mínimo 300 Mbps de throughput de Inspeção SSL;
 - 6.3.1.9.** Deve possuir no mínimo de 4 portas RJ45 100/1000 Ethernet;



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

6.3.1.10. Deverá possuir interface dedicada para fins de gerenciamento do equipamento, atendendo a um dos seguintes padrões: RS-232 (RJ-45 ou DB-9), USB-A, Mini USB ou Micro USB;

7. DOS LOCAIS DE PRESTAÇÃO DO SERVIÇO

Endereço dos Links Dedicados de Internet

a. R. Princesa Isabel, 410 - Santo Amaro, Recife - PE, CEP: 50050-450

Endereços dos enlaces Lan to Lan

b. Enlace de comunicação de dados do tipo Lan to Lan na velocidade de 500 Mbps entre a R. Princesa Isabel, 410 - Santo Amaro, Recife - PE, CEP: 50050-450 e R. da União, 273 - Boa Vista, Recife - PE, CEP: 50050-010

c. Enlace de comunicação de dados do tipo Lan to Lan na velocidade de 500 Mbps entre a R. Princesa Isabel, 410 - Santo Amaro, Recife - PE, CEP: 50050-450 e R. Monte Castelo, 131/166 - Boa Vista, Recife - PE, CEP: 55644-092

d. Enlace de comunicação de dados do tipo Lan to Lan na velocidade de 500 Mbps entre a R. Princesa Isabel, 410 - Santo Amaro, Recife - PE, CEP: 50050-450 e Av. Cais do Apolo, 925, Recife - PE, CEP: 50030-903

8. DOS PRAZOS DE EXECUÇÃO DOS SERVIÇOS

8.1. ELABORAÇÃO DO PLANO DE IMPLANTAÇÃO

8.1.1. A CONTRATADA deverá apresentar um Plano de Implantação em no máximo 10 (dez) dias corridos a partir da assinatura do Contrato.

8.1.2. A CONTRATANTE deverá aprovar o plano de implantação em no máximo 02(dois) dias a partir da sua apresentação.

8.1.3. A execução do Plano de Implantação somente poderá ser iniciada após a sua aprovação pela CONTRATANTE.

8.1.4. O detalhamento do Plano de Implantação deverá conter no mínimo:

a) Cronograma com macro atividades a serem desenvolvidas para a implantação de todos os serviços previstos neste Termo de Referência. O cronograma deverá conter as seguintes informações:



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife – PE

- Identificação dos responsáveis das atividades.
 - Duração das atividades.
 - Sequenciamento das atividades.
- b) Projeto com topologias (física e lógica) da rede, elementos envolvidos, localização dos POPs, faixas de endereçamento IP, detalhamento da gerência, bem como a arquitetura do serviço, incluindo a estratégia de roteamento.

8.2. DA INSTALAÇÃO DOS SERVIÇOS

- 8.2.1.** A CONTRATADA terá até 30 (trinta) dias corridos após a assinatura do contrato para instalar os serviços de comunicação de dados e até 90 (noventa) dias para instalação da solução de segurança, quando demandada.
- 8.2.2.** A instalação do circuito e CPE somente será considerada concluída após a aprovação, pelo Fiscal do Contrato, que ocorrerá em até 5 (cinco) dias corridos após notificação da CONTRATADA.
- 8.2.3.** Todos os equipamentos deverão suportar alimentação com tensão de 110/220 Volts (corrente alternada) bifásica com frequência de 60 Hz.

8.3. DO GERENCIAMENTO DA IMPLANTAÇÃO

- 8.3.1.** Disponibilizar e alocar 1 (um) profissional que será responsável pelo gerenciamento das atividades do projeto de implantação, por parte da CONTRATADA.
- 8.3.2.** Obter informações e esclarecimentos necessários para que possa elaborar o Plano de Implantação do Serviço. Serão abordados e discutidos os seguintes pontos:
- a) Instalação dos circuitos.
 - b) Datas e horários de restrição para implantação.
 - c) Requisitos de infraestrutura necessários para a instalação dos equipamentos.
 - d) Requisitos para a elaboração e entrega do Plano de Implantação do Serviço.
 - e) Serviços que deverão ser configurados na implantação.
 - f) Demais assuntos de interesse correlatos à implantação dos serviços.
- 8.3.3.** Apresentar ao Fiscal do Contrato do CONTRANTE o(s) profissional(is) que atuará(ão) como preposto(s) da empresa para assuntos relativos à execução contratual, e informar ao CONTRANTE o nome completo e o CPF deste(s) preposto(s).

9. CENTRAL DE ATENDIMENTO E SUPORTE TÉCNICO

- 9.1.** A fim de manter os serviços em funcionamento adequado aos parâmetros contratuais, a CONTRATADA deverá:
- 9.1.1.** Possuir um Centro de Operações de Rede (Network Operations Center – NOC)



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por monitorar o funcionamento dos serviços e realizar as ações corretivas necessárias para restabelecer a normalidade dos serviços.

- 9.1.2.** Possuir uma equipe especializada (SOC - Security Operation Center), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável pelo monitoramento, detecção e mitigação de ataques, realizando as ações corretivas necessárias para garantir o bom funcionamento dos serviços.
- 9.1.3.** A CONTRATADA deverá disponibilizar à CONTRATANTE uma Central de Atendimento Técnico, acessível via chamada telefônica gratuita (0800), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por prestar suporte técnico, receber chamados de serviços e prestar informações acerca do andamento destes.
- 9.1.4.** O limite de atuação da CONTRATADA para fins de manutenção, reparo e configuração será a porta LAN de seus roteadores ou switches, de forma a garantir os níveis de serviço contratados.
- 9.1.5.** Enviar à CONTRATANTE, por e-mail, notificações de abertura, andamento e fechamento de chamados, realização de manutenção preventiva ou corretiva e fatos relevantes para a prestação e utilização dos serviços.
- 9.1.6.** Enviar à CONTRATANTE, por e-mail, uma lista de recorrência ("escalation list") contendo os nomes, números de telefone e endereços de e-mail das pessoas que devem ser acionadas em caso de problemas no atendimento técnico. A lista de recorrência deverá ser mantida atualizada e sua versão mais recente deverá ser enviada à CONTRATANTE sempre que houver alteração.
- 9.1.7.** A CONTRATADA deverá iniciar o atendimento no prazo máximo de 1 (uma) hora, contada a partir da data e hora do chamado.
- 9.1.8.** Todo acesso às instalações da CONTRATANTE por pessoal técnico da CONTRATADA, ou de seu preposto, deverá ser previamente agendado.
- 9.1.9.** Manutenções e/ou intervenções programadas nos serviços, quando necessárias, mesmo no caso daquelas que não impliquem inoperância dos serviços contratados ou alteração nas suas características, que necessitem a presença do técnico da CONTRATADA, deverão ser autorizadas pela CONTRATANTE.
- 9.1.10.** Qualquer manutenção e/ou intervenção de caráter emergencial para solução de falhas, inoperâncias e/ou indisponibilidades, verificadas na rede, deverá ser agendada e acordada previamente com a CONTRATANTE.

10. PORTAL DE GERENCIAMENTO E ACOMPANHAMENTO DOS SERVIÇOS

- 10.1.** A CONTRATADA deverá disponibilizar um Portal WEB de gerência, possibilitando a visualização online dos serviços prestados, como também realizar o registro e acompanhamento dos chamados.



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

10.1.1. Consulta e visualização online: O Portal deverá apresentar informações relativas aos ativos de rede utilizados com as seguintes funcionalidades:

- a) Alertas em caso de falhas e anormalidade dos circuitos.
- b) Topologia da rede, incluindo roteadores e circuitos, com a visualização do status de todos os elementos.
- c) Visualização da utilização de banda dos circuitos, de forma diária, semanal e mensal, com a opção de consulta de dados históricos de até 3 (três) meses.
- d) Visualização do consumo de CPU e memória dos roteadores.
- e) Indicação da taxa de perda de pacotes, latência e disponibilidade nos circuitos.
- f) Inventário dos roteadores contendo a configuração física de cada equipamento (interfaces, memória, cpu, etc). modelo e fabricante. endereços IPs e máscaras.

10.1.2. Registro e acompanhamento dos chamados: Permitir o acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços, relativos à pelo menos aos últimos 90 (noventa) dias, incluindo as seguintes informações:

- a) Identificação do registro (número de chamado).
- b) Data e hora de abertura do chamado (registro).
- c) Descrição do problema.
- d) Identificação do reclamante (nome e telefone).
- e) Data e hora de conclusão do atendimento (fechamento do chamado).
- f) Ações realizadas para a solução do problema.

11. GERENCIAMENTO PROATIVO

11.1. A CONTRATADA deverá prover o gerenciamento proativo, com funcionamento 24 horas por dia, 7 (sete) dias na semana, incluindo sábados, domingos e feriados. Entende-se por gerenciamento proativo a capacidade da CONTRATADA de detectar falhas ocorridas nos circuitos (serviços e equipamentos) de forma autônoma e independentemente de notificação por parte da CONTRATANTE. Da mesma forma autônoma a CONTRATADA deve dar início aos procedimentos de correção de falhas e informar imediatamente a CONTRATANTE sobre o evento para sua triagem interna. A CONTRATADA deverá notificar a CONTRATANTE através de telefones e e-mails definidos pela CONTRATANTE no prazo máximo de 25 minutos após a identificação do incidente.

11.2. Gerência exclusiva de relacionamento para acompanhamento, apresentação da evolução e gestão da rede, que fará mensalmente o agendamento e apresentação dos relatórios, através de videoconferência ou por e-mail.

11.3. Atividades realizadas pela equipe responsável pelo gerenciamento proativo:

- a) Gerenciamento individualizado da rede.



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- b) Relatórios mensais sobre a performance da rede.
- c) Relatório Gráfico de indisponibilidade.
- d) Relatório de tráfego de qualidade.
- e) Relatório de Consumo de Banda.
- f) Relatório de Eventos ocorridos.
- g) Relatório de Disponibilidade dos serviços.
- h) Gerenciamento de desempenho proativo.

12. DISPONIBILIDADE

12.1. Índice de Disponibilidade:

12.1.1. Os circuitos de comunicação deverão estar disponíveis 24 horas por dia, todos os dias do ano.

12.1.2. A CONTRATADA deverá garantir disponibilidade mensal de no mínimo, 99,5% para cada circuito fornecido à CONTRATANTE, calculada da seguinte forma:

$$DMA = [(43200 - TTICM) / 43200] \times 100$$

Onde:

TTICM: Tempo Total de Interrupção do Circuito (em minutos) no Mês.

DMA(%): Disponibilidade Mensal Atingida

12.1.3. Para efeito de cálculo de TTICM, será considerado o período em minutos entre o primeiro minuto do primeiro dia e o último minuto do último dia do calendário do mês a que se refere a fatura.

12.1.4. O serviço será considerado indisponível quando não for possível a conexão entre o equipamento da CONTRATANTE e o da CONTRATADA, a partir do registro do chamado técnico na Central de Atendimento da CONTRATADA, sendo considerado disponível após o fechamento do chamado técnico, com a devida anuência da CONTRATANTE, na Central de atendimento da CONTRATADA.

12.1.5. Entende-se como início do atendimento a primeira mensagem trocada pela CONTRATANTE com a CONTRATADA informando a ocorrência ou início da ligação efetuada a central de atendimento da CONTRATADA independentemente do atendimento do operador.

12.1.6. O prazo máximo de recuperação dos circuitos será 2 (duas) horas, todos os dias do mês, inclusive sábados, domingos e feriados.

12.1.7. As indisponibilidades informadas pela gerência e supervisão da CONTRATADA, bem como os registros na Central de Atendimento da CONTRATADA serão validadas pelos



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

sistemas de gerência e supervisão da CONTRATANTE.

12.1.8. No caso de interrupção programada por necessidade da CONTRATANTE, a mesma não afetará o índice de disponibilidade da CONTRATADA.

12.1.9. As interrupções programadas solicitadas pela CONTRATANTE serão previamente combinadas com a CONTRATADA.

12.2. Desconto por interrupção:

12.2.1. Para cada interrupção do circuito que for comprovadamente de responsabilidade da CONTRATADA, será calculado um desconto referente ao tempo de interrupção desse circuito, cujo valor apurado será ressarcido à CONTRATANTE na Nota Fiscal/Fatura dos serviços com vencimento no mês seguinte ao da apuração.

12.2.2. O valor do desconto será obtido a partir do seguinte cálculo:

$$VD = (VC / 43200) \times n$$

Onde:

VD = Valor do Desconto

VC = Valor mensal pago pelo circuito ativo

n = Quantidade de minutos em que o serviço ficou interrompido.

13. NÍVEIS MÍNIMOS DE SERVIÇO

13.1. A CONTRATADA deverá fornecer o serviço com os seguintes níveis mínimos de disponibilidade, latência e taxa máxima de erro, os quais são utilizados para mensurar o desempenho e a qualidade dos circuitos:

Métrica	Nível Mínimo de Serviço
Disponibilidade do link de Internet e Lan to Lan	$\geq 99,5\%$

14. DAS OBRIGAÇÕES

14.1. OBRIGAÇÕES DA CONTRATANTE

14.1.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta.

14.1.2. Comunicar oficialmente à CONTRATADA sobre quaisquer falhas verificadas na fiscalização do cumprimento dos serviços prestados.



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 14.1.3.** Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção.
 - 14.1.4.** Efetuar o pagamento devido pela execução do(s) serviço(s) dentro do prazo estipulado, desde que cumpridas todas as formalidades e exigências contratuais.
 - 14.1.5.** Acompanhar as visitas, inspeções, reuniões solicitadas pela CONTRATADA.
 - 14.1.6.** Prestar, por meio do Fiscal do Contrato, as informações e os esclarecimentos pertinentes ao(s) serviço(s) contratado(s) que venham a ser solicitados pela CONTRATADA.
 - 14.1.7.** Registrar os incidentes e problemas ocorridos durante a execução do Contrato.
 - 14.1.8.** Proporcionar os recursos necessários, técnicos e logísticos, dentro dos locais de instalação dos equipamentos para que a CONTRATADA possa executar os serviços conforme as especificações estabelecidas no Termo de Referência.
 - 14.1.9.** Permitir acesso dos empregados da CONTRATADA, desde que devidamente credenciados, às suas dependências para a realização dos serviços.
 - 14.1.10.** Aplicar as sanções previstas, assegurando à CONTRATADA o contraditório e à ampla defesa.
- 14.2. OBRIGAÇÕES DA CONTRATADA**
- 14.2.1.** Prestar os esclarecimentos que forem solicitados pelo CONTRATANTE, bem como dar ciência ao mesmo, imediatamente e por escrito, de qualquer anormalidade que verificar.
 - 14.2.2.** Comunicar imediatamente ao CONTRATANTE qualquer alteração ocorrida na conta bancária, endereço e outras informações necessárias para recebimento de correspondências e pagamento.
 - 14.2.3.** Responsabilizar-se pelo exato cumprimento de todas as obrigações e exigências decorrentes da legislação trabalhista e previdenciária, ficando claro inexistir entre seus empregados e o CONTRATANTE vínculo empregatício ou de qualquer outra natureza, razão pela qual correrão por conta exclusiva da CONTRATADA todos os ônus decorrentes de rescisões de contratos de trabalho e atos de subordinação de seu pessoal.
 - 14.2.4.** Arcar com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a ser devidos em decorrência da execução do serviço contratado, bem como custos relativos ao deslocamento e estada de seus profissionais, caso exista.
 - 14.2.5.** Manter, durante a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação exigidas em razão da natureza das atividades prestadas e do certame licitatório.
 - 14.2.6.** Fazer diagnóstico das falhas no serviço relatadas pelo CONTRATANTE dentro do prazo estipulado.
 - 14.2.7.** Providenciar a recuperação de falhas na prestação do serviço, comunicadas pelo CONTRATANTE mantendo-o informado sobre as ações efetivadas até a completa normalização da prestação do serviço.



CÂMARA MUNICIPAL DO RECIFE

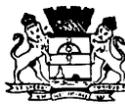
Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

- 14.2.8.** Respeitar o sistema de segurança do CONTRATANTE e fornecer todas as informações solicitadas por ele.
- 14.2.9.** Credenciar junto ao CONTRATANTE um representante, para prestar esclarecimentos e atender às reclamações que porventura surgirem durante a execução do contrato.
- 14.2.10.** O CONTRATANTE não aceitará a transferência de responsabilidade da CONTRATADA para terceiros.
- 14.2.11.** Prestar o serviço contratado conforme especificações, prazos e demais condições estabelecidas no Termo de Referência.
- 14.2.12.** Utilizar melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas neste Contrato e no Termo de Referência.
- 14.2.13.** Reportar formal e imediatamente ao Fiscal do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução do(s) serviço(s)
- 14.2.14.** Atender e prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da área de tecnologia da Informação do CONTRATANTE, referentes a qualquer problema detectado ou ao andamento de atividades previstas.
- 14.2.15.** Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas neste instrumento, caso os prazos, indicadores e condições não sejam cumpridos.
- 14.2.16.** Manter seus profissionais nas dependências do CONTRATANTE adequadamente trajados e identificados com uso permanente de crachá, com foto e nome visível.
- 14.2.17.** Manter-se, durante toda a execução do contrato, em conformidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- 14.2.18.** A CONTRATADA deverá garantir a segurança das informações da CONTRATANTE e se compromete em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do órgão no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

15. QUALIFICAÇÃO TÉCNICA

- 15.1.** As licitantes deverão comprovar para fins de qualificação técnica através da apresentação dos seguintes documentos:
 - 15.1.1.** Apresentar certificado de autorização para exploração de SCM (Serviço de Comunicação Multimídia) emitido pela ANATEL.
 - 15.1.2.** Atestado de capacidade técnica-operacional, em nome da licitante, expedido por pessoa jurídica de direito público ou privado, que comprovem a execução de no mínimo 12 meses, em contrato único ou separado, serviços de solução de segurança de perímetro contemplando o hardware, software, licenciamento, implantação, configuração, garantia, atualizações e suporte técnico, conforme exigências deste



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

Termo de Referência.

15.1.2.1. Comprovação de que possui, mediante contrato em vigor, autorização de Concessionária de Energia local de Pernambuco – CELPE – para utilização de seus postes para construção de redes de Telecomunicações, em conformidade com o REGULAMENTO CONJUNTO PARA COMPARTILHAMENTO DE INFRA-ESTRUTURA ENTRE OS SETORES DE ENERGIA ELÉTRICA, TELECOMUNICAÇÕES E PETRÓLEO, Resolução Conjunta nº 001 de 24/11/1999.

15.1.2.2. O(s) atestado(s) deverão conter, no mínimo, as seguintes informações:

- a) Dados da empresa licitante: nome, CNPJ.
- b) Dados da empresa cliente: nome, razão social, CNPJ, endereço.
- c) Descrição dos serviços prestados com dados que permitam identificar a compatibilidade e similaridade com o objeto da licitação, incluindo as quantidades e taxas de transmissão dos serviços.
- d) Grau de satisfação do cliente, com manifestação expressa do signatário, quanto à qualidade dos serviços prestados.
- e) Dados do emissor do atestado: nome, cargo, telefone e e-mail de contato.
- f) Local, data de emissão e assinatura do emissor.

15.1.3. Apresentar certificado de homologação da ANATEL referente aos equipamentos contemplados na solução.

15.1.4. Atestado de capacidade técnica-operacional ou a Declaração emitida pelo fabricante da solução de segurança, comprovando que a licitante é apta a instalar, configurar, prestar suporte técnico e ministrar treinamentos das soluções referente a esta contratação;

15.1.5. A licitante deverá ainda apresentar Declaração de que possuirá, no ato da assinatura do contrato:

- a) 1 (um) Gerente de Projeto, que será o responsável pela gestão de entrega da solução, devendo ser um profissional em nível superior com graduação e/ou especialização comprovada em telecomunicações ou com Certificação Profissional PMP. O mesmo não poderá ser substituído sem autorização da CONTRATANTE.
- b) 1 (um) Responsável Técnico, devendo ser um profissional com certificação técnica oficial do Fabricante da solução de segurança ofertada. Não será aceito a indicação do mesmo profissional indicado como Gerente de Projeto.

16. DA FORMAÇÃO DO PREÇO DOS SERVIÇOS

16.1. O preço dos serviços deverá ser obtido através da formulação das planilhas abaixo:

Lote 1	Descrição e Especificações	Quantidade	Valor mensal	Valor total (12 meses)
1	Fornecimento de link de acesso dedicado à Internet na velocidade de 1 Gbps, incluindo gerenciamento proativo e proteção contra ataques do tipo DDoS	1		
2	Fornecimento de enlaces dedicados Lan to Lan na velocidade de 500 Mbps	3		



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

3	Fornecimento de solução de segurança composto de firewall de nova geração com SD-WAN para a saída de internet	1		
---	---	---	--	--



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

4	Fornecimento de solução de segurança composto de firewall de nova geração com SD-WAN para os enlaces Lan-to-Lan	3		
---	---	---	--	--



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

Lote 2	Descrição e Especificações	Quantidade	Valor mensal	Valor total (12 meses)
1	Fornecimento de link de acesso dedicado à Internet na velocidade de 1 Gbps, incluindo gerenciamento proativo e proteção contra ataques do tipo DDoS	1		
2	Fornecimento de enlaces dedicados Lan to Lan na velocidade de 500 Mbps	3		
VALOR TOTAL 12 MESES				

16.2. Obter-se-á o valor anual dos serviços através da multiplicação do valor mensal por 12 meses.

Ex. **Valor Total Mensal Estimado dos Serviços: R\$ 00.000,00 x 12 meses**
= Valor Total Anual Estimado dos Serviços: R\$ 000.000,00

17. DO PRAZO DE ENTREGA DOS EQUIPAMENTOS E IMPLANTAÇÃO DO SERVIÇO

17.1. A CONTRATADA terá até 30 (trinta) dias corridos após a assinatura do contrato para instalar os serviços de comunicação de dados e até 90 (noventa) dias para instalação da solução de segurança, quando demandada.

17.2. Do Suporte Técnico: Serão realizados pelos técnicos que ficarão na base da empresa contratada e esse suporte técnico deverá ser acionado sempre que houver necessidade do atendimento, podendo ser realizado por meio do whatsapp, telefone, e-mail;

17.3. Da substituição dos Equipamentos: Durante o contrato sempre que ocorrer a quebra, defeito, falha ou qualquer problema que impeça a utilização do equipamento, a empresa deverá substituí-lo de imediato sem que haja problemas de interrupção do trabalho do setor que estiver usando o equipamento; A substituição imediata do equipamento deve ocorrer em até 4(quatro) horas.

17.4. Equipamentos Backup: Para cada item locado a empresa deverá ter para disponibilidade imediata de 2 (dois) equipamentos com as mesmas configurações.

18. DO PRAZO DE VIGÊNCIA DO CONTRATO

18.1. O Contrato terá vigência de 30 (trinta) meses, contados da assinatura do termo de contrato, por força dos créditos orçamentários, podendo ser prorrogado a critério da administração, nos termos da lei.

18.2. Conforme previsto no inciso II ou IV do art. 57 da Lei n 8.666/93

19. DO PAGAMENTO

19.1. O pagamento dar-se-á mensalmente, pelo Departamento de Finanças da Câmara Municipal do Recife, de acordo com a comprovação da prestação dos serviços correspondentes a cada



CÂMARA MUNICIPAL DO RECIFE

Divisão de Informática

Rua Princesa Isabel, 410 - Boa Vista - Recife - PE

mês, e será efetuado até o 5º (quinto) dia do mês subsequente ao vencido, mediante a apresentação, pela empresa contratada, da nota fiscal devidamente atestada pelo Fiscal do Contrato, a ser designado através de Termo do Primeiro Secretário.

Recife, 16 de Fevereiro de 2023

Ricardo Williams Paixão Ferraz
Diretor da Divisão de Informática