



Câmara Municipal de Curitiba

PREGÃO ELETRÔNICO Nº 004/2023
PROCESSO ADMINISTRATIVO Nº 00090/2023

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

- 1.1. Contratação de empresas especializadas para prestação de serviços continuados de link dedicado de comunicação de dados com a Internet incluindo soluções de segurança da informação, serviço de monitoramento, central de segurança (SOC) e gerenciamento dos serviços.

2. JUSTIFICATIVA

- 2.1. A contratação de 2 Links de Internet, juntamente com um conjunto de segurança disposto de 2 *firewalls* de próxima Geração e barreira de segurança contra ataques de *Distributed Deny of Service* (DDoS) visa atender as necessidades de telecomunicações da Câmara Municipal de Curitiba com os diversos órgãos públicos e empresas terceirizadas a ela vinculados, bem como acesso e publicação de informações pertinentes além de acesso à rede mundial de computadores - Internet.
- 2.2. O objetivo é uma solução de alto desempenho para atender a demanda atual de qualidade, disponibilidade para futuras expansões, padronização, convergência de tecnologia e de serviços, segurança, eficiência e otimização de custos, evolução tecnológica, aumento de produtividade, flexibilidade do uso dos recursos conforme necessidades e gerenciamento proativo centralizado com garantia de disponibilidade e segurança. Não podemos dispor apenas de um ponto de acesso pois, numa eventual falha de um ponto, os sistemas, serviços e o acesso à Internet ficarão indisponíveis. Em um mundo onde cada vez mais a agilidade das informações e o tempo são preciosos, para além da necessidade de conectividade ininterrupta, uma falha dessas pode trazer prejuízos imensuráveis que podem prejudicar a imagem da Câmara Municipal de Curitiba, e impedir a correta execução das atividades fins da instituição, prejudicando a prestação do serviço público.
- 2.3. Hoje a ligação com a Internet é fundamental para o bom andamento dos trabalhos da casa, para inúmeros propósitos, tais como, acesso dos vereadores, servidores e visitantes pela Wi-Fi, acesso de todos os servidores para consultas ligadas diretamente a execução de seu serviço, envio e recebimento de e-mails, envio de arquivos a órgãos de controle (como TCE, Receita federal), consultas a processos judiciais e administrativos, trabalho remoto, além do acesso a diversos sistemas internos da casa, que se baseiam na oferta de serviço em nuvem, que se utiliza da Internet como canal de provimento de acesso.
- 2.4. Ademais o *link* garante acesso dos cidadãos à página institucional da Câmara Municipal, que conta com milhares de acessos diários, e disponibiliza uma série de informações de interesse público, como as transmissões *on-line* das sessões plenárias, consultas ao portal da transparência, notícias da Câmara, dados dos vereadores, proposições, ordem do dia, legislação municipal, presença dos vereadores, atas das comissões permanentes e diversas outras.
- 2.5. É importante registrar que já houve casos de indisponibilidade de acesso à Internet que perduraram por horas, e até dias em uma situação extraordinária, quando a Câmara Municipal mantinha apenas um link de Internet contratado. Estas situações geraram inúmeras reclamações e prejuízos intangíveis que não ocorreriam num cenário em que houvesse um segundo link de redundância disponível, como é o caso que se pretende agora nesta solicitação de contratação. Esta prática condiz com o foco na alta disponibilidade de serviços, resistência a falhas e garantia de funcionamento das atividades da instituição.
- 2.6. Faz-se necessário que o link contratado seja de fornecedores diferentes, aumentando a segurança e diminuindo o risco de indisponibilidade.
- 2.7. Considerando o acesso à Internet como serviço continuado essencial, tanto como o de água ou luz, esta contratação é primordial. Portanto, todo este projeto volta-se para uma



Câmara Municipal de Curitiba

- apurada especificação de equipamentos e serviços, buscando aqueles que tragam o melhor benefício tanto para aplicação imediata quanto futura segundo as necessidades da Câmara Municipal. Além disso, foram considerados os mecanismos precisos para garantir e fiscalizar a eficiência dos fornecedores na implementação das soluções necessárias.
- 2.8. A especificação dos *firewalls* aqui proposta permite a segurança das informações, dos acessos e da manutenção da disponibilidade dos serviços como um todo, através da prevenção de ataques por crackers, inclusive ataques mais elaborados como o DDoS. A redundância e a alta disponibilidade entre estes dois firewalls visa manter pelo menos um dos caminhos de acesso, e proteção, sempre ativo. No caso de falha do link ou equipamento de comunicação, mantém-se de toda forma a disponibilidade dos serviços de rede da instituição. Estes equipamentos do tipo firewall conseguem examinar pacotes da rede de forma muito eficiente, oferecendo proteção mais abrangente e proativa, realizando atualizações de segurança diárias e mecanismos de defesa de última geração.
- 2.9. O método de proteção em camadas consiste em criar várias camadas de proteção distintas e complementares, sendo cada camada atuando de forma especializada em algum componente de segurança.
- 2.10. Grande parte dos serviços prestados pela Câmara Municipal de Curitiba são oferecidos por meio da Internet. Uma das vantagens da Internet é oferecer facilidades como disponibilidade e presença em qualquer lugar. Mas isto também traz a possibilidade de incidentes de segurança, os quais estão crescendo, mundialmente, ano a ano. Os danos causados através dos incidentes de segurança são roubo de informações e valores, indisponibilidade de serviços, destruição de dados, danos à imagem, dentre outros.
- 2.11. O tratamento das ameaças e o gerenciamento da segurança da informação é um desafio para a Câmara Municipal de Curitiba porque:
- 2.11.1. Existem soluções com diferentes fabricantes o que leva a consoles heterogêneos de monitoração que oferecem visões isoladas sobre o estado de segurança do ambiente. Levando a um aumento considerável à uma análise e resposta a um incidente;
 - 2.11.2. Estas análises isoladas levam a uma alta taxa de falsos positivos;
 - 2.11.3. Os analistas precisam interpretar os dados e precisam correlacionar os eventos reportados pelas diferentes soluções, o que leva tempo e pode resultar em um falso positivo;
 - 2.11.4. Existe a obrigatoriedade de estar em conformidade com os órgãos regulamentadores e com as normas de auditoria.
- 2.12. Assim, a Câmara Municipal de Curitiba busca atingir a excelência na segurança para as soluções e ambientes tecnológicos que utiliza. O nível de segurança exigido no tratamento dos seus ativos de informação, com vistas a garantir a confidencialidade, integridade e disponibilidade (CID), será alcançado através da contratação de serviços gerenciados de segurança da informação.
- 2.13. As soluções tradicionais de segurança da informação requerem que as empresas disponham de mão de obra altamente especializada e dedicada na área de segurança, além de investimentos elevados e contínuos em soluções de segurança. A mão de obra especializada em segurança é difícil de contratar ou manter. Por outro lado, os investimentos necessários em soluções de segurança muitas vezes não são realizados de forma sistemática e não conseguem acompanhar a dinâmica do setor.
- 2.14. O *Security Information and Event Management* (SIEM), visa melhorar o modelo de proteção adotado atualmente, minimizando o problema de sobrecarga das equipes, tanto de fiscalização contratual, quanto de gerenciamento da solução.
- 2.15. A gestão da solução atual, com a multiplicidade de equipamentos, traz um custo elevado de integração, operação e atualização. A concentração de alguns serviços em equipamentos que possuem essas funcionalidades como acessórias tende a reduzir custos de contratação e operação do ambiente de segurança.
- 2.16. Com a contratação do SIEM, a Câmara Municipal de Curitiba conseguirá:
- 2.16.1. Entregar escalabilidade elástica e *time to value* rápido;
 - 2.16.2. Correlacionar atividades no ambiente informático para identificar vulnerabilidades e ameaças, priorizando incidentes;
 - 2.16.3. Realizar a análise em tempo real para identificar com precisão as ameaças;



Câmara Municipal de Curitiba

- 2.16.4. Atender os requisitos de auditoria e de conformidade;
- 2.16.5. Ter a seu dispor a equipe da CONTRATADA, com *expertise* de Segurança;
- 2.16.6. Reduzir custos no gerenciamento de Segurança;
- 2.16.7. Aumentar a produtividade interna, com possibilidade de alocação de recursos em outros segmentos;
- 2.16.8. Atender às exigências regulatórias de governança;
- 2.16.9. Proteger seus dados, garantindo a segurança e a integridade.

3. ALINHAMENTO ESTRATÉGICO

- 3.1. A contratação desta solução de TIC colabora para o alcance dos objetivos estratégicos da DTIC:
 - 3.1.1. O presente projeto vem ao encontro ao Planejamento Estratégico da Diretoria de Tecnologia da Informação e Comunicação (2021/2022) - que em seus Objetivos Estratégicos nº 01 e 05 orienta para: "Aprimorar experiência do usuário" e "Prover alta disponibilidade de serviços";
 - 3.1.2. Da mesma forma, este projeto corrobora com o Objetivo Estratégico 07, que visa "Aprimorar a eficiência operacional". Para a equipe da Diretoria de Tecnologia da Informação e Comunicação, retira-se a carga gerada pelo desenvolvimento e manutenção da solução que não faz parte da essência estratégica da Câmara, para os quais existem fornecedores especializados que podem disponibilizá-lo de forma mais eficiente, diminuindo a dependência de recursos e habilidades técnicas e elevando o nível de qualidade na entrega dos serviços. Assegura-se também a estrutura tecnológica de suporte aos processos de trabalho da Câmara.

4. DESCRIÇÃO DA SOLUÇÃO DE TIC

- 4.1. Os bens e serviços que compõem a solução de TIC são listados na [Tabela 1](#):

LOTE 01		
Item	Descrição	Quantidade
I	Link de dados dedicado	01 (um)
II	Anti-DDoS	01 (um)
III	Next-Generation Firewall	02 (dois)
IV	Security Information and Event Management (SIEM):	
	Fornecimento de licenças de uso de solução corporativa de SIEM SaaS com gerência em nuvem	01 (um)
	Fornecimento de licenças de EPS com gerência em nuvem SaaS	1.000 (um mil) EPS por mês
	Serviço de gerenciamento da solução SIEM	01 (um)
VII	Security Information and Event Management (SIEM): Cobrança sobre o volume sazonal adicional de EPS	Até 200 (duzentos) EPS por mês
LOTE 02		
Item	Descrição	Quantidade
I	Link de dados dedicado	01 (um)
II	Anti-DDoS	01 (um)



Câmara Municipal de Curitiba

Tabela 1: Descrição do serviço

4.2. Do parcelamento do objeto:

- 4.2.1. Optou-se pelo parcelamento do objeto para que seja possível obter as melhores condições comerciais para cada tipo de serviço demandado e assegurar alta disponibilidade do serviço de conectividade da Contratante pelo fornecimento de link por operadoras diferentes.
- 4.2.2. Os licitantes poderão habilitar-se em ambos os lotes, porém somente será adjudicado um licitante para cada lote, sendo o vencedor do Lote 1 inabilitado para a participação do Lote 2.
- 4.3. A solução de Link de dados dedicado (Item I, Lotes 1 e 2) refere-se à conexão à internet por enlace de fibra óptica desde o *backbone* da operadora até as instalações da Contratante, com capacidades de transmissão e número de IPs públicos disponíveis de acordo com a necessidade da Contratante.
 - 4.3.1. Nos enlaces fornecidos nos Lotes 1 e 2 não poderá haver conflito ou sobreposição das rotas de lançamento das fibras em suas últimas milhas, para haver assim a redundância e disponibilidade dos links;
- 4.4. A solução de Anti-DDoS (Item II, Lotes 1 e 2) refere-se ao serviço de monitoramento para detecção e mitigação de ataques volumétricos no link de Internet, com gerenciamento proativo e geração de relatórios de acordo com a necessidade da Contratante.
- 4.5. A solução de *Next-Generation Firewall* (Item III, Lote 1) refere-se ao *appliance* de segurança de borda, incluindo proteção contra ameaças, segurança nas conexões e gerenciamento centralizado;
- 4.6. A empresa vencedora do Lote 1 deverá operacionalizar a alta disponibilidade de conexão à Internet para a Contratante utilizando os Links de dados contratados nos Lotes 1 e 2 por meio dos *Next-Generation Firewall*.
- 4.7. A solução de SIEM (Item IV, Lote 1) refere-se ao serviço de monitoramento e detecção de ameaças, contemplando as seguintes atividades: Engenharia de correlação, *Streaming Analytics*, Detecção Comportamental, Análise de Incidentes, Notificação de Incidentes e prestação de serviços de profissionais para atuar no ambiente da CONTRATANTE.

5. DURAÇÃO DO CONTRATO

- 5.1. Considerando o caráter continuado do serviço e para que seja possível obter as melhores condições comerciais para a contratação, o fornecimento terá vigência de 60 meses, podendo ser prorrogado mediante termo aditivo por iguais e sucessivos períodos até o limite de 120 meses estabelecido no art. 107 da Lei nº 14.133/2021.

6. QUALIFICAÇÃO TÉCNICA

- 6.1. A empresa deverá comprovar, por meio de um ou mais atestados de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, com a identificação da empresa ou órgão público, atestando que a licitante prestou ou está prestando, sem qualquer restrição, durante o período de, no mínimo, 12 (doze) meses, serviços com características compatíveis com o objeto deste Termo de Referência, ou seja:

6.1.1. Para o LOTE 1:

- 6.1.1.1. Ter instalado e mantido *link* dedicado para acesso à Internet, com quantitativo mínimo de 512 Mbps;
- 6.1.1.2. Ter prestado serviço Anti-DdoS;
- 6.1.1.3. Ter fornecido solução de *Next-Generation Firewall* (NFGW).

6.1.2. Para o LOTE 2:

- 6.1.2.1. Ter instalado e mantido *link* dedicado para acesso à Internet, com quantitativo mínimo de 512 Mbps;
- 6.1.2.2. Ter prestado serviço Anti-DdoS.

6.1.3. O atestado deve conter:

- 6.1.3.1. Identificação da pessoa jurídica emitente com seu endereço, bem como o nome, telefone e o cargo do signatário;
- 6.1.3.2. Discriminação do serviço prestado;
- 6.1.3.3. Volume ou quantidade de serviços realizados;



Câmara Municipal de Curitiba

- 6.1.3.4. Período de realização dos serviços;
- 6.1.3.5. Caracterização do bom desempenho da licitante, sem ressalvas desabonadoras quanto ao fornecimento/serviço;
- 6.1.3.6. Outros dados característicos se houver;
- 6.1.4. A arrematante poderá disponibilizar todas as informações que entender necessárias à comprovação da legitimidade do atestado, tais como contratos, notas de empenho ou notas fiscais, etc.
- 6.1.5. A ausência de algum dos requisitos do atestado ou dúvidas com relação ao seu conteúdo não o invalidarão se a informação puder ser obtida por diligência ou por meio de outros documentos.
- 6.1.6. Não serão admitidos atestados emitidos por empresas pertencentes ao mesmo grupo econômico da licitante. Consideram-se pertencentes ao mesmo grupo econômico as entidades que embora tendo, cada uma delas, personalidades jurídicas próprias, mantiverem, entre si, direta ou indiretamente, relação de controle (art. 1.098 do Código Civil), ou estiverem sob o controle, direção ou administração, direta ou indireta, de outra pessoa física ou jurídica em comum;
- 6.1.7. Será admitido o somatório de atestados.
- 6.2. A proponente deve declarar que todos os equipamentos ofertados são novos, de primeiro uso e os modelos cotados não estão sofrendo processo de descontinuação, e caso ocorram serão substituídos por novos modelos de mesma especificação ou superior, sem custo adicional, bem como, que garante as atualizações corretivas e evolutivas dos programas durante todo o período contratado, sem custos;
- 6.3. Deverá comprovar, até a assinatura do contrato, que possui certificação técnica da solução ofertada, comprovando a capacitação técnica dos profissionais que serão responsáveis pelas tarefas de instalação, configuração e suporte dos produtos, mediante a entrega de cópia do certificado técnico destes profissionais.
- 6.4. Deverá apresentar carta de parceria com o fabricante do *Next-Generation Firewall* (NFGW) que comprove que está habilitado a comercializar e a operar seus produtos.
- 6.5. Deverá apresentar, junto com a proposta técnica, qual a topologia utilizada para mitigação de ataques DDoS sobre o circuito de dados fornecido.
- 6.6. Deverá ser apresentado folhetos de dados, manuais e outros meios necessários para comprovar o atendimento ao Edital.

7. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

7.1. Item I - Link de dados dedicado

- 7.1.1. O serviço de acesso à internet compreende a instalação, configuração, ativação e gerenciamento proativo do circuito;
- 7.1.2. Os links de dados deverão ser fornecidos por operadoras distintas, ou seja, o vencedor do Lote 1 não poderá atender ao Lote 2.
- 7.1.3. Possuir velocidade simétrica de 500 Mbps de conexão à internet;
- 7.1.4. Prover conexão à rede corporativa da CONTRATANTE, por meio de 2 interfaces do tipo Gigabit Ethernet, operando em velocidade de 1Gbps, com conector RJ-45, em conformidade com a norma IEEE 802.3ab (1000Base-T) para garantir a alta disponibilidade (HA) entre as unidades de Firewall;
- 7.1.5. O acesso deverá ser exclusivo e dedicado à CONTRATANTE, não podendo haver compartilhamento com outros usuários e empresas;
- 7.1.6. Obedecer às recomendações elaboradas pela *Electronic Industries Alliance/Telecommunications Industry Association* (EIA/TIA) e pela Associação Brasileira de Normas Técnicas (ABNT) para provimento de serviços de acesso à Internet (*Internet Service Providers*);
- 7.1.7. Ser provido obrigatoriamente por meio de uma infraestrutura de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso;
- 7.1.8. Prover todos os recursos e equipamentos necessários à prestação dos serviços, tais como: modems, conversores, roteadores e outros correlatos;
- 7.1.9. Ser implementado por meio de uma única porta de acesso na velocidade total contratada, sendo vedada a utilização de múltiplos links físicos de forma a se obter essa velocidade;



Câmara Municipal de Curitiba

- 7.1.10. Suportar os protocolos IPv4 e IPv6, inclusive nos equipamentos fornecidos pela CONTRATADA;
- 7.1.11. O *backbone* IP da CONTRATADA deve ter saída com destino direto a outros provedores de *backbone* IP nacionais, com banda de 15 Gbps no mínimo.
- 7.1.12. Caso a CONTRATANTE se torne um *Autonomous System* (AS) durante a vigência do contrato, a CONTRATADA deverá configurar o uso do protocolo *Border Gateway Protocol* (BGP) em seus equipamentos, para funcionamento do roteamento de pacotes entre as operadoras do Lote 1 e Lote 2;
- 7.1.13. Não possuir limites nem restrições à quantidade de dados trafegados, tais como "*traffic shaping*";
- 7.1.14. Disponibilizar 1 endereço IPv4 roteável na Internet;
- 7.1.15. Fornecer, quando necessário, um bloco de endereços IPv6 roteáveis na Internet, bem como apoio técnico para transição e implementação deste protocolo nos IPs de borda;
- 7.1.16. Disponibilizar serviço de *Domain Name Resolution* (DNS) primário e secundário, para IPv4 e IPv6, da operadora, capaz de resolver direta e reversamente endereços de internet, para registro como *forwarder* nos servidores de DNS da CONTRATANTE;
- 7.1.17. Ser gerenciado contra falhas da operadora, de acordo com, no mínimo, as seguintes condições:
 - 7.1.17.1. 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;
 - 7.1.17.2. Disponibilizar informações sobre os serviços de acesso à internet por meio de um portal de monitoramento, com acesso restrito à CONTRATANTE, utilizando protocolo seguro (HTTPS), contendo estatísticas de desempenho e de disponibilidade do acesso;
 - 7.1.17.3. Possibilitar que a equipe técnica da CONTRATANTE realize consultas no portal de monitoramento, bem como visualizar relatórios das informações de desempenho dos serviços contratados;
- 7.1.18. Ser provido por roteador e demais ativos de rede, a serem instalados nas dependências do *Data Center* principal da CONTRATANTE, com, no mínimo, as seguintes características:
 - 7.1.18.1. Ser dimensionado para garantir, os termos de desempenho e disponibilidade, os Acordos de Níveis de Serviço (ANS) elencados no [Item 9](#) deste termo;
 - 7.1.18.2. Possuir uma interface Gigabit Ethernet - WAN;
 - 7.1.18.3. Possuir duas interfaces Gigabit Ethernet - LAN, com conector RJ-45, em conformidade com o padrão IEEE 802.3ab (1000Base-T);
 - 7.1.18.4. Possuir duas interfaces Gigabit Ethernet - LAN padrão SFP, compatível com o padrão 1000BASE-LX e 2 *transceivers* 1000BASE-LX de forma a possibilitar a utilização destas interfaces e interoperabilidade com a infraestrutura da CONTRATANTE;
 - 7.1.18.5. Suportar configuração de 50 *Virtual Local Area Networks* (VLAN), em conformidade com o padrão IEEE 802.1q;
 - 7.1.18.6. Suportar *Network Address Translation* (NAT) estático e dinâmico;
 - 7.1.18.7. Suportar *Border Gateway Protocol* (BGP);
 - 7.1.18.8. Suportar *Simple Network Management Protocol* (SNMP) v2c e v3, para o sistema de gerência da rede da CONTRATANTE;
 - 7.1.18.9. Suportar protocolo de syslog, para envio de *logs* ao sistema de segurança da rede da CONTRATANTE;
 - 7.1.18.10. Ser gerenciável remotamente (via *Secure Shell* (SSH) ou telnet) e via porta console;
 - 7.1.18.11. Ser instalado com a última versão de *firmware* homologado pelo respectivo fabricante e atualizado constantemente pela CONTRATADA;



Câmara Municipal de Curitiba

- 7.1.18.12. 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”.
- 7.1.19. A instalação e manutenção do roteador, NGFWs e demais ativos de rede deverão ser realizados pela CONTRATADA sem ônus adicional à CONTRATANTE;
- 7.1.20. A CONTRATADA não poderá:
 - 7.1.20.1. 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;
 - 7.1.20.2. Não implementar qualquer tipo de cache transparente, a menos que tenha expressa concordância da CONTRATANTE.
- 7.1.21. O vendedor do Lote 1 deverá fornecer croqui com o caminho do cabo de fibra ótica e posteamento utilizado da operadora até o [Site 1](#) da CONTRATANTE;
- 7.1.22. O vencedor do Lote 2 deverá fornecer croqui com o caminho do cabo de fibra ótica e posteamento utilizado da operadora até o [Site 2](#) da CONTRATANTE
- 7.1.23. Nos enlaces fornecidos nos Lotes 1 e 2, na última milha não poderá haver conflito ou sobreposição de elementos de infraestrutura (tais como postes, caminhos subterrâneos, etc) em suas rotas de lançamento, para haver assim a redundância e disponibilidade dos links;
 - 7.1.23.1. Caso um dos vencedores de um dos Lotes já possua um enlace de fibra óptica instalado na Contratante, não será necessário alterar ou relançar a fibra. Neste caso, o outro vencedor deverá apresentar uma rota de última milha evitando sobreposição com a rota já existente.
 - 7.1.23.2. Caso os vencedores não possuam enlaces instalados na Contratante, o vencedor do Lote 2 deverá apresentar uma rota de última milha evitando sobreposição com a rota apresentada no croqui do vencedor do Lote 1.
 - 7.1.23.3. As licitantes, ao elaborarem suas propostas, podem prever rotas adicionais e participar do certame com um valor adequado às rotas previstas. Desta forma, garante-se que não haja sobreposição de rotas entre Lotes 1 e 2.
- 7.1.24. Os licitantes, quer seja a primeira ou segunda vencedoras, não poderão utilizar elementos da infraestrutura da outra (fibra, roteadores, conversores, última milha, *backbones* etc.). Os links terão total independência e a falha em um não poderá afetar o outro.

7.2. Item II - Anti-DDoS

- 7.2.1. Para proteção deste acesso corporativo A CONTRATADA deverá disponibilizar proteção contra ataques de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques *Denial of Service* (DoS) e *Distributed Denial of Service* (DDoS);
- 7.2.2. A CONTRATADA, e/ou sua empresa terceirizada e prestadora de serviços, deve possuir infraestrutura própria de mitigação com capacidade para conter ataques de grande volume, sendo eles de origem nacional ou internacional. Entende-se por infraestrutura própria de mitigação a existência de equipamentos instalados no *backbone* com objetivo de bloquear o tráfego malicioso, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DDoS;
- 7.2.3. A CONTRATADA deverá possuir pelo menos 2 centros de limpeza, sendo um nacional e outro internacional, com a capacidade de mitigação total de 100 Gbps (cem gigabits por segundo).
- 7.2.4. Não serão aceitas soluções que contemplem equipamentos de mitigação no ambiente da CONTRATANTE, portanto, toda a infraestrutura de mitigação deverá ser instalada obrigatoriamente no *backbone* da CONTRATADA;
- 7.2.5. A técnica Anti-DDoS utilizada deverá ser por métrica de volumetria, não podendo haver restrições por volume de tráfego analisado;
- 7.2.6. A solução Anti-DDoS deverá prover o serviço de mitigação de ataques de negação de serviço (DoS) para o circuito de conectividade IP dedicada à Internet, sejam eles distribuídos (DDoS) ou não;



Câmara Municipal de Curitiba

- 7.2.7. Não haverá custo adicional por volume de mitigação de ataques (DDoS) nos IPs monitorados;
- 7.2.8. O ataque deve ser mitigado separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis;
- 7.2.9. 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;
- 7.2.10. A solução deverá possuir funcionalidades de monitoramento, detecção e mitigação de ataques, mantidas em operação ininterrupta durante as 24 horas do dia, nos 7 dias da semana, no período de vigência contratual;
- 7.2.11. Em casos de ataques não detectados pela solução, quando identificados pela CONTRATANTE, deverão ser mitigados imediatamente pela CONTRATADA após a abertura de chamado através da Central de Atendimento sempre como um chamado com Severidade Crítica (de acordo com a [Tabela 3](#)), e deverá realizá-la, sem nenhum ônus ao CONTRATANTE.
- 7.2.12. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATANTE.
- 7.2.13. O serviço deve prover suporte à mitigação automática de ataques, utilizando múltiplas técnicas incluindo, mas não se restringindo a: Allowlists, Blocklists, limitação de taxa de tráfego, descarte de pacotes malformados, técnicas de mitigação de ataques aos protocolos HTTP, NTP e DNS, bloqueio por localização geográfica de endereços IP.
- 7.2.14. O serviço deve prover também análise de tráfego baseado em reputação de endereços IP, possuindo base de informações própria, que pode ser gerada durante a filtragem de ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.
- 7.2.15. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, para protocolo IPv4, incluindo, mas não se restringindo aos seguintes:
 - 7.2.15.1. Ataques de inundação (*Bandwidth Flood*), incluindo *Flood* de UDP e ICMP;
 - 7.2.15.2. Ataques à pilha TCP, incluindo mal-uso das *Flags* TCP, ataques de RST e FIN, SYN *Flood* e TCP *Idle Resets*;
 - 7.2.15.3. Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
 - 7.2.15.4. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP *Spoofing*);
 - 7.2.15.5. Ataques à camada de aplicação, incluindo protocolos HTTP, DNS, NTP, dentre outros;
 - 7.2.15.6. O serviço deve ser capaz de analisar e aprender o comportamento do tráfego para criar automaticamente parâmetros de bloqueio (Limite de conexão HTTP, TCP, UDP, etc.).
 - 7.2.15.7. O serviço deve ser capaz de detectar anomalias no tráfego, ataques ainda não conhecidos e criar bloqueios em tempo real sem intervenção manual do administrador.
 - 7.2.15.8. A CONTRATADA deve realizar a mitigação de ataques e limpeza do tráfego ilegítimo sem prejudicar ou impedir o tráfego legítimo, seja ele originado de uma ou mais fontes.
 - 7.2.15.9. A solução deve ter serviço de atualização de assinaturas de ataques das soluções de detecção e mitigação.
 - 7.2.15.10. Realizar autenticação de conexão TCP, quando do recebimento de pacotes syn.
 - 7.2.15.11. Ataques denominados de “*Command-and-Control*”, *Point of Sale Malware*, *Remote Access Trojans* (RATs) via *feed* atualizado diariamente.
 - 7.2.15.12. Deve possuir bloqueio de Query de DNS, resposta de query DNS baseado em domínio pré-cadastrado para autenticação e checagem de flag de



Câmara Municipal de Curitiba

- recursão DNS.
- 7.2.15.13. Deve possuir DNS Blocklist;
- 7.2.15.14. RegEx para registros ou “*flags* de recursão”.
- 7.2.15.15. Possuir mecanismos de quando bloquear um ataque por expressão regular DNS, selecionar se bloqueia apenas o ataque ou o host temporariamente.
- 7.2.15.16. Prevenir que host válidos sejam adicionados a blocklist por engano.
- 7.2.16. Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de borda da CONTRATADA;
- 7.2.17. A solução deve permitir a proteção, no mínimo, do tráfego dos *backbone*, serviços web (HTTP/HTTPS), DNS, VPN, FTP e correio eletrônico;
- 7.2.18. A CONTRATADA deverá disponibilizar relatórios mensais de mitigação de ataques ou portal na internet para acompanhamento destes relatórios, contendo no mínimo horário de início do ataque, horário de início de ação de mitigação, horário de sucesso da mitigação e horário de fim do ataque.

7.3. Item III - Next-Generation Firewall

7.3.1. Características Gerais

- 7.3.1.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em *appliance* com funcionalidades de *Next Generation Firewall* (NGFW), console de gerência e monitoração;
- 7.3.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 7.3.1.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no *site* do fabricante em listas de *end-of-life* ou *end-of-sale*;
- 7.3.1.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 7.3.1.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos *appliances* desde que atendam a todos os requisitos desta especificação;
- 7.3.1.6. A solução deve ser composta por *hardware* e *software* do mesmo fabricante;
- 7.3.1.7. O gerenciamento deverá ser feito sem a necessidade de servidores de gerenciamento no ambiente da CONTRATANTE.
- 7.3.1.8. A solução deve possuir certificação ANATEL;
- 7.3.1.9. Deverá possuir e estar licenciado pelo período de todo o contrato vigente com o órgão público com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusão (IPS), VPN IPsec e SSL, Controle de Aplicações, Balanceamento Inteligente e Virtualização.

7.3.2. Requisitos Físicos e de Performance

- 7.3.2.1. *Throughput* mínimo de 60 Gbps com a funcionalidade de *firewall* habilitada, independente do tamanho do pacote, para IPv4 e IPv6;
- 7.3.2.2. *Throughput* mínimo de 12 Gbps de IPS;
- 7.3.2.3. *Throughput* mínimo de 7 Gbps de Inspeção SSL;
- 7.3.2.4. *Throughput* mínimo de 10 Gbps 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 e Anti-Spyware.
 - 7.3.2.4.1. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
- 7.3.2.5. Suporte a 8 milhões de conexões simultâneas;
- 7.3.2.6. Suporte a 450.000 novas conexões por segundo;



Câmara Municipal de Curitiba

- 7.3.2.7. *Throughput* de 45 Gbps de VPN IPSec;
- 7.3.2.8. Estar licenciado para, ou suportar sem o uso de licença, 2.000 túneis de VPN IPsec *Site-to-Site (Gateway-to-Gateway)* simultâneos;
- 7.3.2.9. Estar licenciado para, ou suportar sem o uso de licença, 50.000 túneis de clientes VPN IPsec (*Client-to-Gateway*) simultâneos;
- 7.3.2.10. Suporte a 2.000 conexões de clientes VPN SSL simultâneos;
- 7.3.2.11. *Throughput* de 4 Gbps de VPN SSL;
- 7.3.2.12. 16 interfaces Gigabit Ethernet 1000BASE-T com conectores RJ-45;
- 7.3.2.13. 8 interfaces Gigabit Ethernet SFP 1000BASE-X, sendo que todas as interfaces devem ser entregues populadas, sem custo adicional, com os respectivos *transceivers* do tipo 1000Base-LX;
- 7.3.2.14. 2 interfaces 10 Gigabit Ethernet SFP+ 10GBASE-X, devendo ser fornecidos os *transceivers* do tipo 10GBASE-LR ou 10GBASE-SR, sem custo adicional, apenas sob demanda da CONTRATANTE;
- 7.3.2.15. 2 interfaces 25 Gigabit Ethernet SFP28, devendo ser fornecidos os *transceivers* do tipo 25GBASE-LR ou 25GBASE-SR, sem custo adicional, apenas sob demanda da CONTRATANTE;
- 7.3.2.16. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 5 sistemas virtuais lógicos (Contextos) por *appliance*;
- 7.3.2.17. Permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
- 7.3.2.18. Fontes de alimentação redundantes, internas ao equipamento, 100-240 VAC e com suporte para troca com o equipamento em funcionamento (*hot swappable*);
- 7.3.2.19. Altura máxima de 1U para montagem em rack padrão 19", acompanhado de todos os acessórios para perfeita fixação;
- 7.3.2.20. Os equipamentos (*cluster*) devem ser entregues em configuração de alta disponibilidade e com todas as licenças necessárias para a configuração em modo ativo/ativo.
- 7.3.3. Funcionalidades de Rede e Firewall
 - 7.3.3.1. O gerenciamento da solução deve suportar acesso via SSH, cliente WEB (HTTPS);
 - 7.3.3.2. Suporte a 1024 VLANs Tags 802.1q;
 - 7.3.3.3. Suporte a agregação de links 802.3ad e LACP;
 - 7.3.3.4. Suporte a *Policy based routing* ou *Policy based forwarding*;
 - 7.3.3.5. Suporte a roteamento multicast;
 - 7.3.3.6. Suporte a DHCP Cliente, Server e Relay;
 - 7.3.3.7. Suporte a Jumbo Frames;
 - 7.3.3.8. Suporte a sub-interfaces ethernet lógicas;
 - 7.3.3.9. Suporte a NAT dinâmico (Many-to-Many);
 - 7.3.3.10. Suporte a NAT estático (1-to-1);
 - 7.3.3.11. Suporte a NAT estático bidirecional 1-to-1;
 - 7.3.3.12. Suporte a tradução de porta (PAT);
 - 7.3.3.13. Suporte a NAT de Origem e NAT de Destino simultaneamente;
 - 7.3.3.14. Capacidade de combinar NAT de origem e NAT de destino na mesma política
 - 7.3.3.15. Implementar *Network Prefix Translation* (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
 - 7.3.3.16. Suporte a NAT64 e NAT46;
 - 7.3.3.17. Implementar o protocolo ECMP;
 - 7.3.3.18. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
 - 7.3.3.19. Enviar log para sistemas de monitoração externos;
 - 7.3.3.20. Deve haver a opção de enviar logs para os sistemas de monitoração



Câmara Municipal de Curitiba

- externos via protocolo SSL;
- 7.3.3.21. Possuir mecanismos de proteção anti-spoofing;
 - 7.3.3.22. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
 - 7.3.3.23. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
 - 7.3.3.24. Suporte a roteamento assimétrico (*asymmetric routing*);
 - 7.3.3.25. Suporte ao *modo sniffer*, para inspeção via porta espelhada do tráfego de dados da rede;
 - 7.3.3.26. Suporte ao modo Camada 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
 - 7.3.3.27. Suporte ao modo Camada 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
 - 7.3.3.28. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em modo transparente;
 - 7.3.3.29. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB (*Forwarding Information Base*);
 - 7.3.3.30. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
 - 7.3.3.31. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
 - 7.3.3.32. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
 - 7.3.3.33. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
 - 7.3.3.34. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, OpenStack e Kubernetes;
 - 7.3.3.35. A solução deve possuir conectores nativos para integração com nuvens públicas, pelo menos: AWS, Azure e GPC;
 - 7.3.3.36. Deverá possuir integração com tokens para autenticação de dois fatores;
 - 7.3.3.37. Suporte a controles por zonas de segurança;
 - 7.3.3.38. Controles de políticas por porta e protocolo;
 - 7.3.3.39. Controle de políticas por aplicações e categorias de aplicações;
 - 7.3.3.40. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
 - 7.3.3.41. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
 - 7.3.3.42. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (*outbound*);
 - 7.3.3.43. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
 - 7.3.3.44. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
 - 7.3.3.45. Suporte a objetos e regras IPV6;
 - 7.3.3.46. Suporte a objetos e regras multicast;
 - 7.3.3.47. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
- 7.3.4. Funcionalidades de Controle de Aplicações
- 7.3.4.1. Capacidade de reconhecer aplicações, independente de porta e protocolo;
 - 7.3.4.2. Possibilitar a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
 - 7.3.4.3. Reconhecer pelo menos 4.000 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto,



Câmara Municipal de Curitiba

- update de software, protocolos de rede, VoIP, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 7.3.4.4. Deverá possuir, pelo menos, 15 categorias para classificação de aplicações;
- 7.3.4.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, google chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle db, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
- 7.3.4.6. Deve inspecionar o payload do pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 7.3.4.7. Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
- 7.3.4.8. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- 7.3.4.9. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 7.3.4.10. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
- 7.3.4.11. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 7.3.4.12. Atualizar a base de assinaturas de aplicações automaticamente;
- 7.3.4.13. Possuir integração com Microsoft Active Directory e LDAP, para identificação de usuários e grupos sem a necessidade de instalação de agente no Controlador do Domínio, nem nas estações dos usuários;
- 7.3.4.14. Permitir controle de banda (*traffic shaping*) baseado em aplicações;
- 7.3.4.15. Permitir adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- 7.3.4.16. Suporte a múltiplos métodos de identificação e classificação das aplicações, por, pelo menos, checagem de assinaturas e decodificação de protocolos;
- 7.3.4.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
- 7.3.4.18. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 7.3.4.19. Deve alertar o usuário, em Português do Brasil, quando uma aplicação for bloqueada;
- 7.3.4.20. Possibilitar a diferenciação de tráfegos Peer2Peer, Proxies e Instant Messaging, possuindo granularidade de controle/políticas para os mesmos. Por exemplo, permitir a aplicação Hangouts chat e bloquear a chamada de vídeo da mesma aplicação;
- 7.3.4.21. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube;
- 7.3.4.22. Deve permitir forçar o uso de portas específicas para determinadas aplicações;
- 7.3.5. Funcionalidades de Prevenção de Intrusão e Ameaças
- 7.3.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção



Câmara Municipal de Curitiba

- devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio *appliance* de firewall;
- 7.3.5.2. Incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 7.3.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- 7.3.5.4. Implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
- 7.3.5.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
- 7.3.5.6. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 7.3.5.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
- 7.3.5.8. Suporte a granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 7.3.5.9. Permitir o bloqueio de vulnerabilidades;
- 7.3.5.10. Permitir o bloqueio de exploits conhecidos;
- 7.3.5.11. Deve incluir proteção contra ataques de negação de serviços;
- 7.3.5.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood;
- 7.3.5.13. Detectar e bloquear a origem de *port scans*;
- 7.3.5.14. Bloquear ataques efetuados por *worms* conhecidos;
- 7.3.5.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- 7.3.5.16. Possuir assinaturas para bloqueio de ataques de *buffer overflow*;
- 7.3.5.17. Possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 7.3.5.18. Permitir o uso de operadores de negação na criação de assinaturas customizadas de IPS ou Anti-Spyware, permitindo a criação de exceções com granularidade nas configurações;
- 7.3.5.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 7.3.5.20. Identificar e bloquear comunicação com *botnets*;
- 7.3.5.21. 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;
- 7.3.5.22. Possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 7.3.5.23. Os eventos devem identificar o país de onde partiu a ameaça;
- 7.3.5.24. Incluir proteção contra vírus em conteúdo HTML e *javascript*, *software* espião (*spyware*) e *worms*;
- 7.3.5.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 7.3.5.26. Possibilitar a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do *firewall* considerando: 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 usuário, origem, destino, zonas de segurança;
- 7.3.5.27. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de *malwares* desconhecidos;
- 7.3.5.28. A solução deve ter capacidade de enviar artefatos suspeitos para serem



Câmara Municipal de Curitiba

- executados em ambiente controlado na nuvem do fabricante;
- 7.3.5.29. Suporte a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 7.3.5.30. Permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
- 7.3.6. Funcionalidades de Proteção Contra Ameaças Avançadas
- 7.3.6.1. Possuir funções de Antivírus e Anti-Spyware;
- 7.3.6.2. Possuir Antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP;
- 7.3.6.3. Permitir o bloqueio de *malwares* (*adware*, *spyware*, *hijackers*, *keyloggers*, entre outros);
- 7.3.6.4. Dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de *malware*, ao invés de simplesmente realizar a análise baseada em assinaturas.
- 7.3.6.5. Permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;
- 7.3.6.6. Permitir o bloqueio de download de arquivos por tamanho;
- 7.3.6.7. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
- 7.3.6.8. Dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros.
- 7.3.6.9. Deve ser possível criar políticas de bloqueio de malware utilizando serviços de terceiros, onde o firewall receberá uma lista de hashes maliciosos.
- 7.3.6.10. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
- 7.3.6.11. A solução de *sandbox* deve ser capaz de criar assinaturas e ainda as incluir na base de Antivírus do firewall, prevenindo a reincidência do ataque;
- 7.3.6.12. A solução de *sandbox* deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente;
- 7.3.6.13. Dentre as análises efetuadas, a solução deve suportar Antivírus, consulta na nuvem, emulação de código, *sandboxing* e verificação de chamada de *call-back*;
- 7.3.6.14. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de *sandbox*. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento.
- 7.3.7. Funcionalidades de Filtro de Conteúdo
- 7.3.7.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 7.3.7.2. Possibilitar a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- 7.3.7.3. Capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- 7.3.7.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
- 7.3.7.5. Capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 7.3.7.6. Possuir base ou cache de URLs local no *appliance* ou em nuvem do próprio



Câmara Municipal de Curitiba

- 7.3.7.7. fabricante, evitando *delay* de comunicação/validação das URLs;
- 7.3.7.8. Possuir pelo menos 70 categorias de URLs;
- 7.3.7.9. Possuir a função de exclusão de URLs do bloqueio, por categoria;
- 7.3.7.10. Permitir a customização de página de bloqueio;
- 7.3.7.11. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um *site* potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o *site*);
- 7.3.7.12. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção *Safe Search* estar habilitada no navegador do usuário;
- 7.3.7.13. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de *botnets* conhecidas;
- 7.3.7.14. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;
- 7.3.7.15. Além do *Explicit Web Proxy*, suportar *proxy Web* transparente;
- 7.3.8. Funcionalidade de Identificação de Usuários
 - 7.3.8.1. Capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory e base de dados local;
 - 7.3.8.2. Possuir integração com Microsoft Active Directory, LDAP e RADIUS, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
 - 7.3.8.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
 - 7.3.8.4. Deve possuir integração com Microsoft Active Directory e LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando *Single Sign-On* (SSO). Essa funcionalidade não deve possuir limites licenciados de usuários;
 - 7.3.8.5. 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*);
 - 7.3.8.6. Suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
 - 7.3.8.7. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 7.3.9. Funcionalidade de Filtro de Dados
 - 7.3.9.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
 - 7.3.9.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
 - 7.3.9.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 7.3.10. Funcionalidade de Geolocalização
 - 7.3.10.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
 - 7.3.10.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
- 7.3.11. Funcionalidade de QoS, *Traffic Shapping* e Priorização de Tráfego
 - 7.3.11.1. Permitir ou negar aplicações que possam ter tráfego de dados excessivo (como Youtube, Ustream, entre outros), com a finalidade de controlar o



Câmara Municipal de Curitiba

- consumo excessivo de banda controlando-as por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo *streaming*;
- 7.3.11.2. Suporte a criação de políticas de QoS e *Traffic Shaping* por endereço de origem, destino, porta e por usuário e grupo;
 - 7.3.11.3. Suportar a criação de políticas de QoS e *Traffic Shaping* por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
 - 7.3.11.4. O QoS deve possibilitar a definição de tráfego com banda garantida, banda máxima e por fila de prioridade;
 - 7.3.11.5. Suportar priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
 - 7.3.11.6. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
 - 7.3.11.7. Suportar modificação de valores DSCP para o Diffserv;
 - 7.3.11.8. Suportar priorização de tráfego usando informação de ToS (*Type of Service*);
 - 7.3.11.9. Disponibilizar estatísticas em tempo real para classes de QoS ou *Traffic Shaping*;
 - 7.3.11.10. Suporte a QoS (*Traffic shaping*), em interface agregadas ou redundantes;
- 7.3.12. Funcionalidades de VPN
- 7.3.12.1. Suporte a VPN *Site-to-Site* e *Client-To-Site*;
 - 7.3.12.2. Suporte a IPsec VPN;
 - 7.3.12.3. Suporte a SSL VPN;
 - 7.3.12.4. A VPN IPsec deve suportar 3DES;
 - 7.3.12.5. A VPN IPsec deve suportar Autenticação MD5 e SHA-1;
 - 7.3.12.6. A VPN IPsec deve suportar Diffie-Hellman Group 1, Group 2, Group 5, Group 14 e Group 21;
 - 7.3.12.7. A VPN IPsec deve suportar algoritmo *Internet Key Exchange* (IKE v1 e v2);
 - 7.3.12.8. A VPN IPsec deve suportar AES 128, 192 e 256 (*Advanced Encryption Standard*);
 - 7.3.12.9. A VPN IPsec deve suportar Autenticação via certificado IKE PKI;
 - 7.3.12.10. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
 - 7.3.12.11. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
 - 7.3.12.12. Permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
 - 7.3.12.13. Atribuição de DNS nos clientes remotos de VPN;
 - 7.3.12.14. Permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
 - 7.3.12.15. Suporte a autenticação via AD/LDAP, Secure ID, certificado e base de usuários local;
 - 7.3.12.16. Suporte a leitura e verificação de CRL (*Certificate Revocation List*);
 - 7.3.12.17. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
 - 7.3.12.18. Permitir que a conexão com a VPN seja estabelecida das seguintes forma: Antes da autenticação, após a autenticação, e sob demanda do usuário;
 - 7.3.12.19. O agente de VPN SSL ou IPsec *client-to-site* deve ser compatível com: Ubuntu 18.04 ou superior, Windows 10 64 bit, Mac OS X (v10.10 ou superior);
- 7.3.13. Funcionalidades de Balanceamento Inteligente de Links
- 7.3.13.1. A solução deve ser capaz de agregar vários links em uma interface virtual;
 - 7.3.13.2. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços



Câmara Municipal de Curitiba

- de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
- 7.3.13.3. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, *jitter* e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
- 7.3.13.4. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
- 7.3.13.5. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping e HTTP;
- 7.3.13.6. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (*Spillover*).
- 7.3.13.7. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
- 7.3.13.7.1. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
- 7.3.13.7.2. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, *jitter*, perda de pacotes ou largura de banda;
- 7.3.13.7.3. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
- 7.3.13.7.4. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
- 7.3.13.8. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
- 7.3.13.9. Roteamento dinâmico BGP com suporte a IPv6;
- 7.3.13.10. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);
- 7.3.13.11. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade sede;
- 7.3.13.12. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;
- 7.3.13.13. A solução deve possuir recurso para controlar e corrigir erros na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;
- 7.3.13.14. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;



Câmara Municipal de Curitiba

- 7.3.13.15. Deve possibilitar a definição de largura de banda distintas nas interfaces para *download* e *upload*;
- 7.3.13.16. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (*upload* e *download*) e nível de qualidade dos links (perda de pacote, *jitter* e latência);
- 7.3.13.17. Deve implementar balanceamento de link por *hash* do IP de origem;
- 7.3.13.18. Deve implementar balanceamento de link por *hash* do IP de origem e destino;
- 7.3.13.19. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- 7.3.14. Para permitir a migração, importação ou conversão das configurações e arquitetura em uso pela CONTRATANTE, o modelo fornecido deve ser totalmente compatível com o equipamento atualmente em uso:
 - 7.3.14.1. Fortigate 500E, da fabricante Fortinet.
- 7.3.15. Os NGFWs fornecidos devem ser novos, não remanufaturados, sem uso anterior e em linha de produção;
- 7.3.16. Modelos de referência
 - 7.3.16.1. O fato de serem informados modelos de referência não impede que outros fabricantes/fornecedores forneçam equipamentos similares de equivalência técnica igual ou superior, tão somente serve para que os licitantes possam ter parâmetros de comparação dos dados técnicos, e com isso possam formular propostas considerando o mesmo nível técnico.
 - 7.3.16.2. Apresentam-se alguns modelos de referência:
 - 7.3.16.2.1. Fortinet FortiGate 600F

7.4. Item IV - SIEM

- 7.4.1. Características Gerais
 - 7.4.1.1. A solução deverá consolidar eventos de log de dispositivos, terminais e aplicativos distribuídos;
 - 7.4.1.2. A solução deverá correlacionar as informações de diferentes fontes de logs e agregar eventos relacionados a alertas únicos para acelerar a análise e a correção de incidentes;
 - 7.4.1.3. A solução deve ser implementada totalmente no modelo SaaS (*Software as a Service*);
 - 7.4.1.4. A solução deverá ter disponibilidade mensal mínima (em %) de 99,5%;
 - 7.4.1.5. A solução deve ser flexível a períodos de sazonalidade, permitindo aumento da licença quando necessário e retorno ao volume inicial contratado quando o período de sazonalidade finalizar;
 - 7.4.1.5.1. Assim, a solução deverá permitir a recepção de eventos que excedam temporariamente os limites contratados, processando o volume excedente assim que o volume for normalizado. Permitindo assim operar com situações de picos temporários, sem incorrer na perda de eventos;
 - 7.4.1.5.2. A cobrança sobre o volume sazonal será realizada conforme o volume de EPS tratado;
 - 7.4.1.5.3. A cobrança sobre o volume sazonal será realizada conforme o volume de EPS tratado, até o máximo estimado de 200 EPS por mês. A cobrança do volume sazonal será realizada em unidades de 100 EPS.
 - 7.4.1.6. A solução deverá possibilitar a coleta dos logs *on-premises* através da utilização de agentes;
 - 7.4.1.7. Para a coleta de logs, a solução deverá oferecer a possibilidade da utilização de até 10 coletores de eventos que podem ser posicionados de acordo com sua arquitetura de preferência;
 - 7.4.1.8. Os coletores e logs devem fazer a compactação e criptografia dos dados antes do envio dos mesmos à nuvem do SIEM;



Câmara Municipal de Curitiba

- 7.4.1.9. Em caso de coletas de logs que ficam posicionados na nuvem, a coleta deve ser feita diretamente de nuvem da aplicação para a nuvem do SIEM, sem necessidade de transição dos logs pela infraestrutura da CONTRATANTE, desde que a solução em nuvem permita a coleta via integrações por API. Ex.: Office365, AWS;
- 7.4.1.10. A solução deverá segregar logicamente os logs da CONTRANTE dos demais logs de outras CONTRATANTES que utilizem a solução de SIEM SaaS;
- 7.4.1.11. A solução deve possuir monitoria de disponibilidade e infraestrutura 24x7x365;
- 7.4.1.12. Caso a solução seja composta por módulos, a mesma deverá ser de um único fabricante, garantindo assim o suporte da solução, quanto às funcionalidades e integrações e 100% compatíveis;
- 7.4.1.13. A solução deve incluir armazenamento de logs por pelo menos 3 meses online.
- 7.4.1.14. A coleta, normalização e o correlacionamento dos eventos provenientes dos dispositivos monitorados devem ser realizadas próximos ao tempo real;
- 7.4.1.15. Para melhor operação e entendimento dos eventos, estes devem ser normalizados e categorizados em um padrão único que será usado pela solução;
- 7.4.1.16. A solução deverá permitir a definição de metadados customizados/personalizados, para extrair dados existentes na linha de log (*raw*), usando recursos como expressões regulares ou algum recurso gráfico para essa extração;
- 7.4.1.17. Propriedades customizadas poderão ser utilizadas em regras de correlação online e em regras de correlação histórica;
- 7.4.1.18. A solução deverá permitir a agregação de eventos semelhantes;
- 7.4.1.19. A solução deverá atribuir métrica de prioridade para os eventos e para os alertas/incidentes;
- 7.4.1.20. A solução deverá gerar alertas/incidentes com base nas regras definidas previamente;
- 7.4.1.21. A solução deverá permitir armazenar os eventos, inclusive os normalizados, de forma compactada;
- 7.4.1.22. Permitir a análise de eventos baseados em contexto, tais como, usuários, localização geográfica, bem como qualquer outro metadado contido no evento;
- 7.4.1.23. Apresentar painéis gráficos (*dashboards*) com indicativos de situações relacionados à segurança, aplicações e monitoração do próprio sistema;
- 7.4.1.24. Os painéis gráficos (*dashboards*) devem ser customizáveis, por usuário; Permitir a visualização, na interface web, dos eventos relacionados a um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução;
- 7.4.1.25. Enviar notificações relacionadas a um incidente/alerta por e-mail;
- 7.4.1.26. A solução deverá ter, no mínimo, as seguintes formas de coleta de eventos: Syslog (UDP, TCP), Syslog criptografado com TLS, JDBC, SNMP (v1, v2 e v3), Microsoft Event Log, MQ Series client, Arquivos de Log em formato de texto, Kafka, Checkpoint OPSEC/LEA, CISCO NSEL e Juniper NSM Protocol;
- 7.4.1.27. Ter a capacidade de reenviar os log e *flows*, em formato nativo, para outros sistemas em tempo real;
- 7.4.1.28. A solução deverá possuir a capacidade de reenviar eventos já normalizados para outros sistemas de correlacionamento em tempo real;
- 7.4.1.29. A solução deverá permitir a configuração de ofuscação de qualquer parte dos dados recebidos, assim que normalizados;
 - 7.4.1.29.1. A ofuscação de dados deve ser configurada com chaves de criptografia;
- 7.4.1.30. A solução deverá possuir a capacidade de automatizar a resposta a



Câmara Municipal de Curitiba

- incidentes, através da execução de scripts, como ação customizada dentro das regras de correlação;
- 7.4.1.31. A solução deverá possuir a capacidade de customizar e personalizar diferentes *templates* de email que serão enviados como resposta aos incidentes identificados;
 - 7.4.1.32. A solução deverá ser capaz de processar logs em formato JSON, identificando e criando automaticamente os campos comuns do log como metadados para aquele tipo de log;
 - 7.4.1.33. A solução deverá ser capaz de processar logs em formato JSON permitindo a definição manual/customizada de metadados, usando a estrutura/caminho do JSON para a definição da propriedade;
 - 7.4.1.34. A solução deverá permitir a criação de metadados com nomes personalizados, de livre escolha, permitindo a referência desse metadado em pesquisas e regras de correlações;
 - 7.4.1.35. A solução deverá permitir a definição de metadados customizados/personalizados, para extrair dados de uma linha de log (*raw*), usando recursos como expressões regulares, JSON, LEEF e CEF, a partir de dados RAW previamente armazenados na solução de correlação, permitindo usar esses dados em pesquisas de eventos.
- 7.4.2. Características do componente de coleta de logs
- 7.4.2.1. Deverá permitir a compactação e criptografia dos dados para envio dos logs para a nuvem;
 - 7.4.2.2. Deverá permitir realizar a normalização dos dados pré-envio do mesmo para a solução em nuvem;
 - 7.4.2.3. Deverá filtrar e selecionar os eventos que serão inseridos na solução ou que serão retidos na base de dados da solução por períodos previamente definidos;
 - 7.4.2.4. Deverá permitir a criação e alteração de políticas de retenção;
 - 7.4.2.5. Deverá normalizar e categorizar os eventos em um padrão único que será usado pela solução;
 - 7.4.2.6. Deverá possuir suporte nativo para reconhecimento e coleta de, pelo menos, 250 tipos de fontes de dados diferentes;
 - 7.4.2.7. Deverá tratar eventos em formato comprimido (zip, gz, tar.gz), sem a necessidade da descompressão manual;
 - 7.4.2.8. Deverá fazer a agregação de eventos, mostrando a contagem de eventos, quando o mesmo evento ocorrer dentro de um período curto.
 - 7.4.2.9. A opção de realizar ou não a agregação de eventos deve ser configurável;
 - 7.4.2.10. Deverá manter o evento bruto (*raw*) e seus metadados para o armazenamento e consulta futura;
 - 7.4.2.11. Deverá ser capaz de agregar informações sobre localização geográfica dos endereços IP envolvidos no evento, para que a mesma seja usada no correlacionamento;
 - 7.4.2.12. Um único componente da solução deve ser capaz de coletar, processar e normalizar tanto os eventos de segurança e eventos de negócio (não relacionados à segurança);
 - 7.4.2.13. Tanto os eventos de segurança quanto os de negócios devem ser normalizados para um único padrão de eventos;
 - 7.4.2.14. A solução deve permitir a integração de dispositivos ou logs não suportados nativamente;
 - 7.4.2.15. A integração de logs ou dispositivos deve ser realizada na interface web, com o uso de expressões regulares, JSON e recurso similar, sem exigir o uso de linguagens de programação ou scripts, tais como Java, C, TCL/TK, PowerShell, Shell Scripts, etc.
 - 7.4.2.16. A mesma integração deve suportar as seguintes formas de coleta de eventos:
 - 7.4.2.16.1. Syslog (UDP, TCP);
 - 7.4.2.16.2. Syslog criptografado com TLS;



Câmara Municipal de Curitiba

- 7.4.2.16.3. JDBC;
- 7.4.2.16.4. SNMP (v1, v2 e v3);
- 7.4.2.16.5. Microsoft Event Log;
- 7.4.2.16.6. Arquivos de Log em Formato de texto;
- 7.4.2.16.7. Check Point OPSEC/LEA;
- 7.4.2.16.8. CISCO NSEL;
- 7.4.2.16.9. Kafka;
- 7.4.2.16.10. Juniper NSM Protocol.
- 7.4.2.17. A solução deve suportar, nativamente, pelo menos as seguintes fontes de logs:
 - 7.4.2.17.1. Windows;
 - 7.4.2.17.2. Linux;
 - 7.4.2.17.3. IBM/AIX;
 - 7.4.2.17.4. IBM/RACF;
 - 7.4.2.17.5. HP-UX, Solaris;
 - 7.4.2.17.6. Oracle Database;
 - 7.4.2.17.7. IBM/DB2;
 - 7.4.2.17.8. PostgreSQL;
 - 7.4.2.17.9. MS SQL Server;
 - 7.4.2.17.10. Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet e Palo Alto e SonicWall);
 - 7.4.2.17.11. Network IPS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee).
- 7.4.2.18. A solução deve permitir a criação automática de data sources pela detecção do tipo de fonte do log, dentre as nativamente suportadas, enviados via Syslog;
- 7.4.2.19. A solução deve permitir a criação automática de data sources pela detecção do tipo de fonte do log, dentre as tipos de logs customizados na solução, quando enviados via Syslog;
- 7.4.2.20. A solução deve suportar *overlap* de IP, isto é, rotular os eventos para que seja possível gerenciar eventos de fontes de log que estejam em redes diferentes, mas possuem o mesmo endereçamento IP.
- 7.4.3. Características do correlacionamento de logs
 - 7.4.3.1. A solução deve permitir correlacionamento de eventos provenientes das fontes de logs e flows, gerando incidentes de segurança;
 - 7.4.3.2. A solução deve efetuar o correlacionamento dos eventos próximo ao tempo real;
 - 7.4.3.3. A solução deve efetuar o correlacionamento dos *flows* próximo ao tempo real;
 - 7.4.3.4. A solução deve permitir a criação de novas regras e a edição das existentes;
 - 7.4.3.5. A solução deve permitir o correlacionamento de qualquer informação que conste no evento, inclusive informações que não sejam referentes a endereçamento IP, portas, etc, tais como dados financeiros;
 - 7.4.3.6. A solução deve suportar no mínimo 300 regras de correlação especializadas na detecção de incidentes de segurança;
 - 7.4.3.7. A solução deve possuir regras de correlação específicas para regulações/conformidades, com suporte no mínimo a: PCI, ISO 27001 e GDPR/LGPD;
 - 7.4.3.8. A solução deve possuir repositório que ofereça novas regras de correlação especializadas em segurança para atualização e ampliação da capacidade de detecção de incidentes, sem custo adicional;
 - 7.4.3.9. A solução deve permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos/tráfego, quando comparados a outros períodos similares (ex. mesmo período do dia, mesmo dia da semana);
 - 7.4.3.10. A solução deve permitir a criação de regras que identifiquem desvios, em



Câmara Municipal de Curitiba

- qualquer metadado, de limites pré-estabelecidos;
- 7.4.3.11. A solução deve possuir a capacidade de detectar automaticamente padrões de ataques especializados que acontecem ao longo do tempo e não foram previstos ou observados anteriormente;
- 7.4.3.12. A solução deve integrar com ferramentas externas como Nslookup, Whois, Nmap;
- 7.4.3.13. A solução deve permitir o correlacionamento de eventos e alertas com dados existentes em listas (*watchlist*), permitindo também a criação de novas listas e a edição das existentes, de forma automatizada e manual;
- 7.4.3.14. A solução deve possuir a capacidade de fazer o correlacionamento entre eventos e fluxos de rede, NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou qualquer componente adicional ao licenciamento da solução;
- 7.4.3.15. A solução deve ser capaz de correlacionar eventos oriundos de mais de uma fonte, tipo ou localização;
- 7.4.3.16. A solução deve possuir a capacidade de priorizar os eventos e incidentes com base, pelo menos, nos seguintes critérios:
- 7.4.3.17. Severidade e criticidade/relevância do evento ou incidente. Podendo ser utilizada uma combinação desses critérios;
- 7.4.3.18. Os incidentes devem ser agrupados, no mínimo, por:
- 7.4.3.19. Categoria;
- 7.4.3.20. Endereço de origem;
- 7.4.3.21. Endereço de destino;
- 7.4.3.22. A solução deve possuir pelo menos os seguintes tipos de correlação:
- 7.4.3.23. Correlação por regras;
- 7.4.3.24. Extrapolação de um limite (*threshold*);
- 7.4.3.25. Correlação por anomalia e padrão de comportamento;
- 7.4.3.26. Como resultado das regras, deve ser capaz de executar ações automáticas, no mínimo:
- 7.4.3.27. Enviar e-mail;
- 7.4.3.28. Enviar mensagem para o usuário conectado no console;
- 7.4.3.29. Criar um incidente no sistema de *workflow* interno;
- 7.4.3.30. Enviar traps SNMP e popular listas (*watchlist*);
- 7.4.3.31. A solução deve possuir a capacidade de se integrar com pelo menos um ou mais sistemas de inteligência com informações de riscos globais tais como: HP ThreatLink (DVLabs), Symantec DeepSight, Verisign iDefense, IBM X-Force;
- 7.4.3.32. A solução deve possuir a facilidade de usar qualquer metadado dos eventos em uma regra de correlação;
- 7.4.3.33. A solução deve permitir testar as regras de correlação em eventos passados, em período de tempo e escopo bem definidos;
- 7.4.3.34. A correlação histórica deve permitir a escolha do período a ser analisado, atendendo no mínimo a correlação compreendo a análise de 1 dia, 7 dias e 30 dias;
- 7.4.3.35. Regras de correlação histórica devem processar logs e *flows*, gerando alertas quando os eventos/*flows* analisados combinarem com o especificado na regra;
- 7.4.3.36. Uma regra de correlação deve ser capaz de correlacionar eventos de tipos diferentes, de origens diferentes, checando situações como: a ocorrência de uma sequência de diferentes eventos, uma contagem de eventos, a não ocorrência de um eventos após a ocorrência de outro.
- 7.4.4. Características da console de administração e operação
- 7.4.4.1. A solução deverá ser operada exclusivamente pela CONTRATADA.
- 7.4.4.2. A CONTRATADA deverá entregar juntamente com a solução SIEM o serviço de Gerência atuando na Detecção e Triagem de Incidentes;
- 7.4.4.3. O gerenciamento deverá ter como premissa uma abordagem preventiva e reativa, detectando eventos suspeitos e realizando a classificação de



Câmara Municipal de Curitiba

- incidentes de Cibersegurança e informando a CONTRATANTE via relatório a cada evento identificado.
- 7.4.4.4. A CONTRATADA deverá ser responsável por identificar e classificar os eventos de segurança utilizando a ferramenta de SIEM e a CONTRATANTE será responsável pela tratativa do evento no serviço/host indicado no relatório fornecido pela CONTRATADA.
- 7.4.4.5. O Serviço de Gerenciamento deverá ter como tecnologia base o SIEM.
- 7.4.4.6. O Serviço de Gerenciamento deverá disponibilizar para a CONTRATANTE as facilidades:
- 7.4.4.7. Monitoração de eventos;
- 7.4.4.8. Gestão de incidentes;
- 7.4.4.9. Criação de novas regras de correlação e casos de uso e detecção;
- 7.4.4.10. Inteligência de ameaças e conformidade;
- 7.4.4.11. A console de administração e operação, a ser operada pela CONTRATADA, deverá:
- 7.4.4.12. Possuir Interface web única para administração, gerenciamento e operação da solução como um todo
- 7.4.4.13. Possuir acesso controlado e autenticado por usuário;
- 7.4.4.14. Possuir capacidade de integração com bases Microsoft Active Directory, LDAP, TACACS e RADIUS para autenticação de usuários;
- 7.4.4.15. Deve permitir a integração com Single Sign-On que suporte o protocolo SAML 2.0
- 7.4.4.16. Possuir acesso seguro e criptografado à interface web, de forma a garantir a confidencialidade;
- 7.4.4.17. Garantir acesso aos dados e às funcionalidades/ações diferenciadas por perfis de acesso;
- 7.4.4.18. O controle de acesso deve ser configurado na interface web, com capacidade para limitar os recursos da solução a perfis de usuários, conforme critérios definidos pelo administrador;
- 7.4.4.19. O controle de acesso deve permitir a configuração de acesso por perfil às funções de Administração, Incidentes, Configuração de Regras, acesso a atividades de Redes e Logs;
- 7.4.4.20. Permitir visualização de eventos, *flows* de rede e incidentes de segurança em tempo próximo ao real;
- 7.4.4.21. Permitir pesquisa nos eventos históricos, a partir de metadados, fornecendo capacidade de *drill-down*, ou seja, o refinamento da pesquisa a partir da seleção de elementos no resultado, para efetuar nova pesquisa.
- 7.4.4.22. Deve permitir a visualização dos detalhes dos eventos, inclusive o evento original (*raw*), quando aplicável, para análise forense e investigação de incidentes;
- 7.4.4.23. Permitir a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução;
- 7.4.4.24. Possuir a capacidade de criação de novos painéis gráficos (*dashboards*) e alteração dos existentes;
- 7.4.4.25. Possuir a capacidade de visualizar eventos de mais de um tipo de dispositivo na mesma visualização (ex: Firewall, Proxy e anti-vírus na mesma visualização);
- 7.4.4.26. Possuir a capacidade de criação de listas (*watchlist*) e alteração das existentes. Permitindo a inserção dos dados de forma manual, por linha de comando e automática através das regras de correlação;
- 7.4.4.27. Permitir a remoção de dados das listas (*watchlist*) de forma manual, automática através de regras de correlação e pela expiração do tempo de vida da informação;
- 7.4.4.28. Possuir a capacidade de gerenciamento e configuração centralizada de todas as partes distribuídas da solução;
- 7.4.4.29. Possuir a capacidade de atualização de componentes da solução, a partir da console central de administração;



Câmara Municipal de Curitiba

- 7.4.4.30. Possuir a capacidade de restaurar informações de cópia de segurança do banco de dados, configurações e dados, que foram arquivadas previamente pela solução;
 - 7.4.4.31. Permitir a criação de novos tipos de eventos na ferramenta, a fim de integrar logs não suportados nativamente;
 - 7.4.4.32. Permitir a associação manual de eventos já normalizados, mas ainda não categorizados/associados, às categorias, classificações ou tipos de eventos já existentes, ou aos definidos pelo usuário;
 - 7.4.4.33. Para análise dos eventos e *flows* de rede, deve suportar filtros de eventos, usando filtros simples, pesquisa de expressões e buscas avançadas diretamente na base de dados;
 - 7.4.4.34. Deve disponibilizar APIs do tipo webservices, do tipo "RESTful API", para acesso externo à solução, permitindo busca de informações de eventos e *flows*, manipulação de incidentes.
 - 7.4.4.35. Deve suportar o controle de acesso a solução baseado em informações externas a solução, através da validação de atributo do usuário ou grupo que esse faz parte. Deve suportar essa validação de autorização em diretórios LDAP ou Windows Active Directory.
 - 7.4.4.36. Deve suportar API para criação de fontes de logs (*data sources*) por interface ReST, com vistas a automação.
 - 7.4.4.37. Deve permitir a geração de relatórios, contendo múltiplas informações num mesmo relatório, como dados de segurança e rede;
 - 7.4.4.38. Deve permitir a criação de relatórios relacionados a: incidentes, logs, *flows* de rede, vulnerabilidades;
 - 7.4.4.39. Deve possuir relatórios classificados em grupos temáticos, permitindo a criação novos agrupamentos de relatórios pelo usuário;
 - 7.4.4.40. Deve permitir a customização de novos relatórios baseados em dados de Logs, *Flows* de rede, Vulnerabilidades e Incidentes;
 - 7.4.4.41. Deve gerar relatórios de eventos, alertas/incidentes em nível técnico e gerencial os quais devem ter a possibilidade de serem gerados em PDF, HTML, XLS, CSV, XML e RTF/DOC;
 - 7.4.4.42. Os usuários devem poder visualizar apenas os seus próprios relatórios ou relatórios disponibilizados por outros usuários, os administradores devem poder visualizar todos os relatórios;
 - 7.4.4.43. Deve ser possível definir perfis de usuários com permissão/restrição de edição dos modelos de relatórios;
 - 7.4.4.44. Deve ser possível realizar relatórios baseados em dados com IPv6;
 - 7.4.4.45. A funcionalidade de cópia de segurança deve preservar os dados de relatórios;
 - 7.4.4.46. Deve permitir a geração de relatórios que contenham os eventos associados a um incidente detectado por regras de correlação.
- 7.4.5. Para esta contratação, a estimativa de 1.000 EPS foi calculada utilizando os itens mapeados na [Tabela 2](#):

Dimensionamento de EPS	
Item	Tipo de dispositivo
1	Sistemas de núcleo de alto volume. Exemplos: Core Firewalls, Ingress Proxies, Core UTM Firewalls, etc.
2	Sistemas de núcleo de volume médio. Exemplos: Proxies de saída, filtragem da Web de saída, gateways de segurança da Web / e-mail, Edge / Small Firewalls / UTM
3	Infraestrutura de segurança típica.



Câmara Municipal de Curitiba

	Exemplos: IDS / IPS, VPN, balanceadores de carga, NAC, DLP, WAF, DAM, NBAD, CASB, etc.
4	Soluções de autenticação. Exemplos: AD, autenticação, IAM, PIM, PAM, MFA, etc
5	Soluções de serviço de rede. Exemplos: Fontes DHCP, DNS, Virtual / Cloud (isto é, ESX)
6	Soluções IaaS / PaaS. Exemplos: Contas ou <i>hubs</i> IaaS (Amazon AWS, Google, Azure, etc.)
7	Soluções principais de SaaS. Exemplos: O365, Akami, GuardDuty, CloudTrail, etc.
8	Soluções Anti-Malware. Exemplos: Anti-malware ou antivírus, soluções de gateway de e-mail
9	Soluções de criptografia. Exemplos: Gerenciamento de criptografia (repouso, movimento, WDE, etc.) Infraestrutura de chave pública e gerenciamento de certificado.
10	Sistemas Web / Mail. Exemplos: IIS, Apache, Exchange, SendMail, etc
11	Soluções de gerenciamento de estoque. Exemplos: Gerenciamento de endereço IP (IPAM), distribuição de software, gerenciamento de patch, inventário, soluções de gerenciamento de configuração
12	HIPS e soluções de detecção. Exemplos: Soluções de engano (Honeypots), detecção / prevenção de intrusão de host de servidor (HIPS)
13	Soluções Edge SaaS. Exemplos: Soluções SaaS Small / Edge (Salesforce, Box, etc.)
14	Servidor de banco de dados e mainframe. Exemplos: Sistemas de banco de dados e mainframe (Oracle, IBM, iSeries, Microsoft, etc.)
15	Servidores Windows. Exemplos: Servidores de uso geral do sistema operacional Windows
16	Servidores IX e DB. Exemplos: Servidores de uso geral do sistema operacional Linux / Unix
17	Terminais / hosts da estação de trabalho. Exemplos: Detecção e resposta de endpoint (EDR), sistema operacional <i>host</i> do cliente ou fontes Sysmon
18	Sistemas de rede. Exemplos: Roteadores, switches, APs sem fio, controladores, etc.
19	Estações de trabalho. Exemplo: todas as estações de trabalho usando recursos de rede corporativa
20	Servidores no ambiente. Exemplo: todas as instâncias de servidor, incluindo virtual e nuvem / IaaS



Câmara Municipal de Curitiba

21	Usuários ou contas a serem monitorados
22	Data centers ou <i>hubs</i> de coleta

Tabela 2: Itens utilizados no dimensionamento da solução SIEM

7.4.6. Modelos de referência

7.4.6.1. O fato de serem informados modelos de referência não impede que outros fabricantes/fornecedores forneçam equipamentos similares de equivalência técnica igual ou superior, tão somente serve para que os licitantes possam ter parâmetros de comparação dos dados técnicos, e com isso possam formular propostas considerando o mesmo nível técnico.

7.4.6.2. Apresentam-se alguns modelos de referência:

7.4.6.2.1. IBM QRadar on Cloud

7.5. Centro Operacional de Segurança

7.5.1. A CONTRATADA deve disponibilizar um Centro Operacional de Segurança (*Security Operations Center - SOC*) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, ou com custo de ligação local para a cidade de Curitiba, em idioma português brasileiro, durante as 24 horas do dia, nos 7 dias da semana, no período de vigência contratual;

7.5.2. A CONTRATADA deve apresentar, até a assinatura do contrato, comprovação, através de certificado de treinamento oficial, de que o SOC está apto a operar, suportar e gerenciar as soluções de segurança fornecidas.

7.5.2.1. Alternativamente, serão aceitos documentos que comprovem indiretamente a qualificação da equipe do SOC.

7.6. Prazo de execução

7.6.1. O início do processo de instalação e ativação dos serviços deverá ocorrer em até 10 (dez) dias consecutivos após a emissão da Autorização para Prestação de Serviços.

7.6.2. A conclusão de implantação dos serviços contratados, incluindo todas as configurações necessárias para o seu perfeito funcionamento, instalação física e lógica do link, fornecimento e implantação dos NGFWs, regras contra ataques DDoS e ativação do SIEM, deverá ocorrer no prazo máximo de 30 (trinta) dias consecutivos após a emissão da Autorização para Prestação dos Serviços, que poderá ser antecipado conforme necessidade da Contratante, desde que de comum acordo entre as partes.

7.6.2.1. Na impossibilidade, devidamente justificada, do cumprimento do prazo de fornecimento e implantação dos NGFWs estabelecido no Item 7.6.2, a CONTRATADA deverá garantir a prestação de serviços nos moldes atuais com a solução completa, com entrega dos equipamentos novos no prazo de 30 dias consecutivos.

7.6.2.2. Os prazos poderão ser prorrogados por solicitação justificada do adjudicatário e aceita pela Administração, até o limite de 90 dias consecutivos.

7.6.3. Após a implantação dos serviços a equipe de homologação, composta de técnicos da Contratante e com o apoio de técnicos da Contratada, efetuará os testes de conformidade e verificação final.

7.7. Local de execução

7.7.1. Os serviços deverão ser executados nas dependências da Câmara Municipal de Curitiba, localizados nos endereços:

7.7.1.1. **Site 1 (Sala de Telecomunicações):** Rua Barão do Rio Branco, 720 - Centro - CEP: 80010-902 - Curitiba - Paraná - Brasil. Prédio Pátio Central, Térreo;



Câmara Municipal de Curitiba

7.7.1.2. **Site 2 (Sala Técnica):** Rua Barão do Rio Branco, 583 - Centro - CEP: 80010-180 - Curitiba - Paraná - Brasil. Anexo IV, Térreo;

- 7.7.2. Durante a execução do contrato poderá ser solicitada a alteração dos endereços de instalação de acordo com as necessidades da CONTRATANTE, em casos decorrentes de obras civis ou adequações nos ambientes onde estejam instalados os links e demais equipamentos previstos no projeto. Nestes casos a CONTRATADA promoverá sua reinstalação no(s) novo(s) ambiente(s) ou endereço(s) da CONTRATANTE, deixando-os em perfeitas condições de uso e sem custo adicional;

7.8. Transferência de conhecimento

- 7.8.1. A Contratada deverá fazer a transferência de conhecimento de, no mínimo, 40 (quarenta) horas para até 8 funcionários a serem definidos pela Contratante. O repasse de conhecimento visa um treinamento básico de startup das soluções e não um treinamento oficial.
- 7.8.2. A transferência de conhecimento poderá ser feita nas dependências da Contratante, ou poderá ser realizada através de forma online por meio de ferramentas de colaboração.

8. FISCALIZAÇÃO

- 8.1. A execução do contrato será acompanhada e fiscalizada por fiscais administrativos e fiscais técnicos:

Servidor	Matrícula	Fiscal
Aquino Umeo	2296	Fiscal administrativo
Ewerton Cesário Peres	2129	Fiscal técnico
Tarcísio Socher	2146	Fiscal técnico suplente

- 8.2. Aos servidores da Contratante incumbirá acompanhar a prestação dos serviços, determinando à Contratada as providências necessárias ao regular e efetivo cumprimento da obrigação;
- 8.3. O acompanhamento e a fiscalização da execução da contratação consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, podendo ser exercido por um ou mais representantes da Contratante, especialmente designados, na forma do art. 117 da Lei nº 14.133/21;
- 8.4. A Contratante, por intermédio de seu fiscal designado, ficará responsável para acompanhar/fiscalizar a execução dos serviços, que registrará em relatório todas as ocorrências verificadas e determinará as providências necessárias à regularização das falhas ou defeitos observados, conforme dispõe o § 1º, do art. 117, da Lei nº 14.133/21;
- 8.5. A Contratante verificará a adequação dos procedimentos utilizados pela Contratada em relação às exigências da legislação que regulamente ou que venha a regulamentar o objeto deste Termo de Referência;
- 8.6. O recebimento definitivo e aceitação do objeto ficarão a cargo de servidor designado para Fiscal da contratação, obedecendo ao disposto nas alíneas a e b, inciso II do art. 140, da Lei nº 14.133/21, bem como ao disposto no art. 119 da Lei nº 14.133/21;
- 8.7. Os serviços serão recebidos definitivamente após a verificação de sua qualidade e



Câmara Municipal de Curitiba

- adequação, em conformidade com a proposta da Contratada, com a consequente aceitação mediante termo circunstanciado de Atesto de Recebimento;
- 8.8. Os servidores da Contratante somente aceitarão os serviços que forem executados com estrito atendimento às condições expressas neste documento;
 - 8.9. Os serviços poderão ser rejeitados, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser repetidos no prazo fixado pelo servidor responsável, às custas da Contratada, sem prejuízo da aplicação das penalidades cabíveis;
 - 8.10. Quaisquer exigências da fiscalização inerentes ao objeto da contratação deverão ser prontamente atendidas pela Contratada;
 - 8.11. A Contratada, por ocasião da prestação dos serviços, deverá apresentar nota fiscal em que conste a especificação dos serviços prestados, quantidade, preço unitário e valor total;
 - 8.12. A fiscalização será exercida no interesse da Câmara Municipal de Curitiba e não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por quaisquer irregularidades e, na sua ocorrência, não implica corresponsabilidade do Poder Público ou de seus agentes e prepostos;
 - 8.13. As decisões e providências que ultrapassem a competência do servidor serão solicitadas à autoridade competente da Contratante, para adoção das medidas convenientes, consoante disposto no art. 117 da Lei nº 14.133/21;
 - 8.14. A ação ou omissão da Contratante no acompanhamento e fiscalização não exime a Contratada de sua total e exclusiva responsabilidade sobre os produtos oferecidos, o cumprimento dos prazos e quaisquer outras obrigações contratuais ou legais.

9. ACORDO DE NÍVEL DE SERVIÇOS

9.1. Gerenciamento, monitoramento e suporte técnico

- 9.1.1. Após a instalação e ativação, toda a solução contratada estará disponível e será gerenciada e monitorada proativamente pela CONTRATADA durante 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano).
- 9.1.2. No caso de incidentes que comprometam o serviço prestado, a CONTRATADA deverá realizar os procedimentos necessários para recolocar o link de comunicação em seu pleno estado de funcionamento e de uso e deve comunicar à CONTRATANTE.
- 9.1.3. O prazo de início de atuação do monitoramento proativo será de até 30 minutos corridos, contados a partir do horário de detecção do incidente.
- 9.1.4. Fornecer atendimento especializado 24x7 (por vinte e quatro horas nos sete dias da semana), por intermédio de uma central de atendimento, que poderá ser via web, aplicativos de mensagens, telefone ou correio eletrônico (e-mail), todos em língua portuguesa, no Brasil.
- 9.1.5. Os serviços de suporte deverão ser prestados de forma presencial ou remota, dependendo da necessidade ou solicitação da CONTRATANTE.
- 9.2. Os chamados abertos poderão ser referentes a todas as atividades de responsabilidade da CONTRATADA considerando os serviços contratados, englobando, mas não se limitando, a instalação, configuração, recuperação, alteração e remoção de equipamentos, enlaces, roteamento, endereçamento IP, entre outros;
- 9.2.1. Para o Lote 1, inclui-se a gerência completa dos NGFWs;
- 9.3. Os registros dos chamados deverão conter todas as informações relativas ao chamado aberto, como tempo de início e fim de atendimento, identificação do elemento (equipamento, enlace ou serviço) afetado, nome, telefone e e-mail do contato na CONTRATANTE que foi posicionado acerca do serviço, descrição detalhada da resolução do chamado, evidências e orientações para diagnóstico de problemas e na interpretação de *traces*, *dumps* e *logs*;



Câmara Municipal de Curitiba

- 9.4. O prazo de início de atendimento ao chamado técnico será de até 01 hora corrida, contada a partir do horário da abertura do chamado.
- 9.5. Após o início do atendimento, o tempo de solução do problema deverá ser de acordo com a [Tabela 3](#), não devendo ultrapassar os prazos estabelecidos para as respectivas severidades, contados a partir da abertura do chamado técnico.

Severidade	Descrição	Tempo de solução
1 - Crítica	Chamados referentes a situações de emergência ou problemas críticos, caracterizados pela existência de indisponibilidade, ambiente paralisado, impedimento da contratante de cumprir prazos legais em relação a terceiros, problemas que impeçam o fechamento da folha de pagamento ou grave comprometimento dos dados	Até 4 horas
2 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho, paralisação parcial do serviço ou sob risco de parada	Até 8 horas
3 - Média	Chamados associados a incidentes sem paralisação do serviço ou problemas que se apresentem de forma intermitente, incluindo casos em que haja necessidade de substituição de componentes que possuam redundância	Até 12 horas
4 - Baixa	Chamados para esclarecimento de dúvidas, configurações da solução, manutenções programadas e resolução de problemas de baixo risco	Até 24 horas
5 - Programada	Chamados destinados à elaboração de diagnóstico, avaliação e tuning da solução, resolução de problemas, customização de funcionalidades, documentação de procedimentos implementação de procedimentos de evolução de versão de produto e aplicação de melhorias e correções	A ser acordado

Tabela 3: Tabela de severidade e prazos de solução de chamados

- 9.6. Um chamado somente poderá ser fechado após confirmação do responsável da CONTRATANTE e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento.
- 9.7. É de responsabilidade da CONTRATADA a manutenção dos equipamentos, enlases e cabos utilizados para fornecimento do Link, sem ônus para a CONTRATANTE;
- 9.8. Os equipamentos defeituosos, caso não possam ser reparados, deverão ser substituídos pela CONTRATADA, sem ônus para a CONTRATANTE;
- 9.9. Quaisquer modificações e/ou reconfigurações que necessitem ser executados nos equipamentos pela CONTRATADA deverão ser autorizadas e acompanhadas por um responsável da CONTRATANTE;
- 9.10. Disponibilidade do serviço
- 9.10.1. Disponibilidade mensal mínima (em %) de 99,5%;
- 9.10.2. A disponibilidade será aferida mensalmente de acordo com a fórmula de cálculo:
- 9.10.2.1. $IDM = \frac{(T - Ti)}{T} \times 100$, onde:
- 9.10.2.2. **IDM** é o índice de disponibilidade mensal do circuito de internet em %
T é o período de operação (um mês) em minutos
Ti é o somatório dos tempos de inoperância durante o período de operação (um mês) em minutos.
- 9.10.2.3. No caso de inoperância recorrente num período inferior a 3 horas, contado



Câmara Municipal de Curitiba

a partir do restabelecimento do enlace da última inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o enlace estiver totalmente operacional.

- 9.10.2.4. A indisponibilidade de dados de gerência (coleta não realizada, dados não acessíveis, etc.) será considerada como indisponibilidade do serviço, caso isto implique em perda de dados de gerenciamento.
- 9.10.2.5. Os tempos de inoperância serão os tempos em que os enlaces apresentarem problemas. Eles serão obtidos dos chamados abertos no sistema de abertura de chamados técnicos. Somente serão desconsiderados os tempos de inoperância, causados por manutenções programadas com a CONTRATANTE, ressalvados, contudo, os casos fortuitos, de força maior e causas atribuídas a CONTRATANTE.
- 9.10.3. Qualquer interrupção programada PELA CONTRATADA para manutenção preventiva e/ou substituição dos equipamentos e meios utilizados, desde que possa causar interferência no desempenho do serviço prestado, deverá ser comunicada ao CONTRATANTE com antecedência mínima de 3 dias úteis, por meio de correio eletrônico, e somente será realizada com a concordância do CONTRATANTE;
 - 9.10.3.1. Somente serão aceitas interrupções programadas quando as referidas manutenções e/ou ampliações exigirem tecnicamente alterações no(s) circuitos e/ou equipamento(s) responsáveis pela conexão com o CONTRATANTE.
 - 9.10.3.2. Quando o prazo mínimo de 3 dias úteis de comunicação não for atendido, deverá ser concedido desconto por interrupção.

9.11. Relatórios

- 9.11.1. Mensalmente deverá ser disponibilizado à CONTRATANTE, por e-mail ou em portal disponível na Internet, relatório constando os acionamentos técnicos abertos, em andamento e encerrados;
 - 9.11.1.1. O relatório deve conter no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, severidade, nome do responsável do CONTRATANTE pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, tipo do atendimento (remoto ou *on-site*), data e hora de encerramento ou aplicação de solução de contorno e descrição da resolução adotada. O relatório deverá apresentar ainda o índice de disponibilidade do serviço detalhando períodos de indisponibilidade quando houverem;
 - 9.11.1.2. O relatório deverá ser entregue mesmo quando não houver chamados no período;
 - 9.11.1.3. Este relatório é essencial para a elaboração dos atestados de pagamentos mensais, sem os quais poderão ocorrer atrasos, cuja responsabilidade será atribuída à CONTRATADA.
- 9.11.2. Mensalmente deverá ser disponibilizado à CONTRATANTE, por e-mail ou em portal disponível na Internet, relatório constando as ameaças detectadas e/ou mitigadas no serviço de Anti-DDoS;
 - 9.11.2.1. O relatório deve conter no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, severidade, data e hora de ocorrência do incidente, data e hora do início do atendimento, data e hora de encerramento ou aplicação de solução de contorno e descrição da resolução adotada. O relatório deverá apresentar ainda o índice de disponibilidade do serviço detalhando períodos de indisponibilidade quando houverem;
- 9.11.3. Disponibilizar acesso *on-line* a gráficos de utilização do *link* da CONTRATADA.
- 9.11.4. Para o Lote 1, aplicam-se ainda:
 - 9.11.4.1. Mensalmente deverá ser disponibilizado à CONTRATANTE, por e-mail ou em portal disponível na Internet, relatório constando as ameaças detectadas e/ou mitigadas no Firewall;



Câmara Municipal de Curitiba

- 9.11.4.1.1. O relatório deve conter no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, severidade, data e hora de ocorrência do incidente, data e hora do início do atendimento, data e hora de encerramento ou aplicação de solução de contorno e descrição da resolução adotada. O relatório deverá apresentar ainda o índice de disponibilidade do serviço detalhando períodos de indisponibilidade quando houverem;
- 9.11.4.2. Mensalmente deverá ser disponibilizado à CONTRATANTE, por e-mail ou em portal disponível na Internet, relatório constando as ameaças detectadas e/ou mitigadas no Firewall;
 - 9.11.4.2.1. O relatório deve conter no mínimo as seguintes informações: aplicações de risco, *exploits* detectados, *malwares*, *botnets*, *spywares* e dispositivos de rede comprometidos.
- 9.11.4.3. Mensalmente deverá ser disponibilizado à CONTRATANTE, por e-mail ou em portal disponível na Internet, relatório com informações gerenciais e de performance da solução;
 - 9.11.4.3.1. O relatório deve conter no mínimo as seguintes informações: uso de banda, número de sessões, aplicações, categorização e dados de produtividade.
- 9.11.4.4. Mensalmente deverá ser disponibilizado à CONTRATANTE, por e-mail ou em portal disponível na Internet, relatório da solução SIEM contendo:
 - 9.11.4.4.1. Visão de chamados com visão de severidade, grupos, tipos e categorias;
 - 9.11.4.4.2. Acompanhamento de Log Sources mensal;
 - 9.11.4.4.3. Acompanhamento de consumo de licenças;
 - 9.11.4.4.4. Visão de ameaças por mês, magnitude e usuários;
 - 9.11.4.4.5. Visão de eventos com origem e destino;
 - 9.11.4.4.6. Top 10 IPs de origem e destino dos eventos;
 - 9.11.4.4.7. Relatórios de ameaças com as seguintes informações:
 - 9.11.4.4.7.1. Detalhes do incidente (Histórico, localidade e descrição)
 - 9.11.4.4.7.2. Resultado da análise (Recursos afetados, hosts suspeitos e vetor de ataque)
 - 9.11.4.4.7.3. Fatores de mitigação (Recomendações para mitigação)
- 9.11.5. A CONTRATADA terá até o 5º dia útil de cada mês para a disponibilização dos relatórios.

9.12. Glosas

- 9.12.1. A violação de qualquer um dos níveis de serviço, definidos no Termo de Referência, só poderá ser desconsiderada pela CONTRATANTE quando for decorrente de uma das seguintes ocorrências, descritas a seguir:
 - 9.12.1.1. Falha em algum equipamento de propriedade da CONTRATANTE;
 - 9.12.1.2. Falha decorrente de procedimentos operacionais da CONTRATANTE;
 - 9.12.1.3. Falha de qualquer equipamento da CONTRATADA que não possa ser corrigida por inacessibilidade causada pela CONTRATANTE.
- 9.12.2. Ficam estabelecidos os seguintes percentuais de glosas sobre os pagamentos devidos à CONTRATADA quando do descumprimento das metas estabelecidas para os níveis de serviço:
 - 9.12.2.1. 3% do valor mensal dos serviços, para cada dia útil de suspensão ou interrupção, total ou parcial, salvo motivo de força maior ou caso fortuito, dos serviços contratados;
 - 9.12.2.2. 1% do valor mensal dos serviços, para cada ocorrência, por manter funcionário sem qualificação para executar os serviços contratados;
 - 9.12.2.3. 1% do valor mensal dos serviços, para cada ocorrência, por acumular 2 advertências em um período de 6 meses;
 - 9.12.2.4. 0,2% do valor mensal dos serviços, para cada ocorrência, por deixar de prestar quaisquer informações solicitadas no prazo estipulado;
 - 9.12.2.5. 3% do valor mensal dos serviços, para cada ocorrência, por

Página 31 de 37



Câmara Municipal de Curitiba

- descumprimento do [Índice de Disponibilidade Mensal](#) (IDM);
- 9.12.2.6. 3% do valor mensal dos serviços, para cada ocorrência, por descumprimento da disponibilidade mensal mínima da solução de SIEM SaaS, definida no [Item 7.4.1.4](#);
- 9.12.2.7. 10% do valor mensal dos serviços, para cada ocorrência, por indisponibilidade do serviço superior a 4 horas consecutivas, cumulativamente com as glosas previstas nos itens anteriores;
- 9.12.2.8. 0,5% do valor mensal dos serviços, para cada hora ou fração, por atraso nos prazos de início de atendimento e solução dos chamados;
- 9.12.2.9. 10% do valor mensal dos serviços, na ocorrência de descumprimento de qualquer dos níveis de qualidade do serviço definidos no [Item 9](#), por 3 meses consecutivos ou 5 meses intervalados, em um período de 12 meses;
- 9.12.2.10. 1% do valor mensal dos serviços, para cada ocorrência, por atraso na apresentação dos relatórios mensais.
- 9.12.3. O somatório das glosas por descumprimento dos níveis de serviço estará limitado a 70% do valor mensal dos serviços.
- 9.12.4. No caso de aplicação de glosa referente ao mesmo indicador deste Acordo de Níveis de Serviço, durante três meses consecutivos, ou cinco meses intercalados no período de 12 meses, caracterizará inexecução parcial sujeita à aplicação das sanções administrativas previstas no Termo de Referência, inclusive a rescisão contratual.
- 9.12.5. Todas as sanções para o caso de inadimplemento estão limitadas ao valor mensal dos serviços contratados e citados em cada indicador.
- 9.12.6. Os percentuais previstos para o caso de inadimplemento de qualquer atendimento ou serviço corresponde ao percentual de desconto que deverá ser aplicado sobre o valor da fatura referente ao mês em que o nível de serviço não foi atingido.
- 9.12.7. A aplicação de glosas tem caráter educativo e corretivo e não influencia a aplicação das sanções cabíveis por qualquer descumprimento contratual ou outra infração.

10. SANÇÕES

- 10.1. O descumprimento de qualquer condição estabelecida no Termo de Referência, edital, contrato ou instrumento equivalente possibilitará à Câmara Municipal de Curitiba, garantido o contraditório e a ampla defesa, aplicar aos licitantes e à adjudicatária as seguintes penalidades, nos termos da Lei nº 14.133/2021:
- 10.1.1. Advertência;
- 10.1.2. Multa;
- 10.1.3. Impedimento de licitar e contratar;
- 10.1.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública.
- 10.2. As sanções poderão ser aplicadas de forma gradativa, isolada ou cumulativa, e em sua aplicação serão considerados:
- a) a natureza e a gravidade da infração cometida;
- b) as peculiaridades do caso concreto;
- c) as circunstâncias agravantes ou atenuantes;
- d) os danos que provierem da infração para a Administração Pública;
- e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 10.3. A advertência poderá ser aplicada para situações de inexecução parcial do contrato, quando não se justificar a imposição de penalidade mais grave;
- 10.3.1. O fornecedor receberá um comunicado de advertência, sempre que houver a incidência de glosas contratuais em razão de prestação de serviços abaixo do Nível de Serviço acordado com a Administração;
- 10.4. Na aplicação das multas serão observados os seguintes percentuais:
- 10.4.1. 0,5% ao dia sobre o valor adjudicado em caso de atraso no início da execução dos serviços.



Câmara Municipal de Curitiba

- 10.4.2. Após o décimo quinto dia e a critério da CONTRATANTE, no caso de execução com atraso, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.
- 10.4.3. 20% sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no [Item 7.6](#), ou de inexecução parcial da obrigação assumida.
- 10.4.4. 30% sobre o valor adjudicado, em caso de inexecução total da obrigação assumida.
- 10.5. O impedimento de licitar e contratar se dará na forma e nas hipóteses do art. 156, § 4º, da Lei nº 14.133/2021
- 10.6. A declaração de inidoneidade para licitar ou contratar com a Administração Pública se dará na forma e nas hipóteses do art. 156, § 5º, da Lei nº 14.133/2021;
- 10.7. A reabilitação da licitante ou contratada poderá ser admitida na forma do art. 163 da Lei nº 14.133/2021.

11. VISTORIA TÉCNICA

- 11.1. Recomenda-se às licitantes interessadas realizar vistoria técnica, com antecedência mínima de 2 dias úteis da data marcada para abertura do certame licitatório;
- 11.2. A vistoria destina-se ao reconhecimento, pelas empresas, dos locais onde serão implantados os links e equipamentos;
- 11.3. A vistoria deverá ser previamente agendada com a Divisão de Infraestrutura, Telecomunicações e Suporte da CONTRATANTE, dentro do horário de expediente, em dias úteis, das 08h às 12h e das 14h às 18h, pelo e-mail suporte@cmc.pr.gov.br ou pelo telefone (41) 3350-4812, com antecedência mínima de 1 dia útil da data da vistoria;
- 11.4. Não será realizada vistoria sem prévio agendamento ou fora do prazo estabelecido;
- 11.5. A vistoria poderá ser realizada por responsável técnico ou representante da pessoa jurídica interessada em participar da licitação, que deverá comparecer portando documento de identificação pessoal e comprovante de vínculo com a empresa ou de procuração.
 - 11.5.1. A comprovação do vínculo poderá ser feita através do contrato de trabalho, contrato provisório de trabalho, contrato de prestação de serviço ou contrato social da empresa (no caso de sócio ou gerente).
- 11.6. No caso de não realização da vistoria, as licitantes assumirão total concordância com todos os dispositivos constantes neste edital e em seus anexos e com as condições do local, não sendo admitidas, em hipótese alguma, alegações posteriores de desconhecimento sobre os serviços, quantitativos, prazos ou dificuldades técnicas não previstas.

12. OBRIGAÇÕES DA CONTRATADA

- 12.1. Executar os serviços conforme especificações do Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários a execução dos serviços na qualidade e quantidade especificadas no Termo de Referência e em sua proposta;
- 12.2. Promover a instalação e configuração da solução, incluindo todos equipamentos previstos no projeto, nos ambientes da CONTRATANTE, deixando-os em perfeitas condições de uso;
- 12.3. Responsabilizar-se por toda e qualquer despesa, independente da sua natureza, decorrente das instalações supramencionadas;
- 12.4. São de responsabilidade da contratada os seguintes itens: frete, seguro, embalagens, manuais, despesa de transporte ou quaisquer custos relacionados a entrega, instalação e repasse de conhecimento;
- 12.5. Realizar reuniões prévias à instalação antecipadamente agendadas com a Diretoria de Tecnologia da Informação e Comunicação da CONTRATANTE para definição das etapas e cronograma da implantação da solução contratada;
- 12.6. O controle de qualidade dos serviços e materiais utilizados na prestação do serviço;
- 12.7. Disponibilizar, no prazo de 5 (cinco) dias úteis após a assinatura, pela CONTRATADA, da Autorização para Prestação de Serviços, equipe técnica especializada para:



Câmara Municipal de Curitiba

- 12.7.1. Análise das configurações existentes no ambiente produtivo de NGFWs da CONTRATANTE;
- 12.7.2. Validar com a equipe de TI da CONTRATANTE as configurações a serem realizadas nos NGFWs fornecidos;
- 12.7.3. Realizar a migração ou conversão das configurações e aplicá-las nos NGFWs fornecidos garantindo total operacionalidade com o ambiente produtivo atual;
- 12.7.4. A aceitação do fornecimento do Item III está condicionada à efetiva utilização dos NGFWs fornecidos em ambiente produtivo da CONTRATANTE. A aceitação será registrada formalmente pelo Fiscal Técnico da CONTRATANTE.
- 12.8. Ativação da solução SIEM
 - 12.8.1. A CONTRATADA deverá prover o Planejamento do Projeto de Assistência à implementação do SIEM em Nuvem, incluindo:
 - 12.8.1.1. Reunião, a ser realizada por videoconferência, para o alinhamento para planejar e agendar as tarefas do projeto.
 - 12.8.1.2. Confirmação junto a CONTRATANTE das expectativas e funcionalidades a serem implementadas.
 - 12.8.1.3. Garantir que os requisitos ambientais e operacionais para a implementação (logística, hardware, software e infraestrutura) sejam atendidos e, se necessário, fornecer à CONTRATANTE uma lista de atualizações necessárias.
 - 12.8.2. Validar com a equipe de TI da CONTRATANTE a arquitetura da solução e as fontes de log e fluxo para definição dos casos de uso.
 - 12.8.3. A CONTRATADA executará as seguintes tarefas:
 - 12.8.3.1. Ativação da solução de SIEM para a quantidade de EPS que atenda o ambiente detalhado na Tabela 2.
 - 12.8.3.2. Configurar a correlação de tipos de fonte de log no Serviço em Nuvem.
 - 12.8.3.3. Esta atividade incluirá a transferência de conhecimento para o pessoal relevante da CONTRATANTE.
 - 12.8.4. Após a implantação da solução, para casos de inclusão de novos ativos, ficará a cargo da CONTRATANTE realizar o apontamento dos ativos para envio dos logs a solução de SIEM. Mediante prévio alinhamento entre a CONTRATANTE e a CONTRATADA.
 - 12.8.5. Ajuste inicial, que inclui ativação de regras prontas para uso, pesquisas salvas, gráficos de séries temporais acumuladas e relatórios; identificar e remover fontes de ruído; etc).
- 12.9. É obrigatório incluir na proposta técnica a marca e o modelo específico do NGFW ofertado para atendimento das especificações contidas nesse Termo de Referência, juntamente ao(s) catálogo(s) e/ou manual(ais) que comprovem as características requisitadas;
- 12.10. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.
- 12.11. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo de 30 dias consecutivos, os serviços fornecidos em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- 12.12. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os arts. 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990), ficando a CONTRATANTE autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;
- 12.13. Responsabilizar-se pelos atos de seus empregados e danos causados à CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo na execução do presente contrato, arcando com toda e qualquer indenização proveniente de suas ações ou omissões;
- 12.14. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica;



Câmara Municipal de Curitiba

- 12.15. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
- 12.16. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- 12.17. Apresentar, sempre que solicitado, durante a execução do contrato, documentos que comprovem o cumprimento a legislação em vigor quanto às obrigações assumidas;
- 12.18. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços, bem como prestar, prontamente, os esclarecimentos que lhe forem solicitados;
- 12.19. Prestar à CONTRATANTE, sempre que necessário e solicitado, esclarecimentos e informações acerca dos serviços a serem executados e produtos/materiais a serem empregados, fornecendo toda e qualquer orientação que possa ser dada para acompanhamento e apreciação dos mesmos;
- 12.20. Facilitar o acompanhamento e fiscalização da CONTRATANTE sobre a execução dos serviços;
- 12.21. Acatar as recomendações da fiscalização da Câmara Municipal de Curitiba, facilitando a ampla ação desta, com pronto atendimento aos pedidos de esclarecimento porventura solicitados;
- 12.22. Comunicar, por escrito, qualquer anormalidade verificada na execução do objeto e prestar os esclarecimentos necessários;
- 12.23. Comunicar expressamente à CONTRATANTE, a quem deliberar a respeito, toda e qualquer irregularidade observada no objeto da contratação;
- 12.24. Priorizar a utilização de materiais menos perigosos, duráveis, certificados, recicláveis e/ou reutilizáveis, de forma a atender a legislação vigente relativa ao tema;
- 12.25. Assumir inteira responsabilidade pela prestação dos serviços, de acordo com as especificações constantes na proposta e/ou instruções do Edital e seus anexos.
- 12.26. Garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso, durante os procedimentos de instalação e manutenção dos seus equipamentos, bem como durante a operação do serviço;
- 12.27. Submeter-se às normas gerais da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.704/2018, e do Marco Civil da Internet, Lei LEI Nº 12.965, e assumir responsabilidade sobre todos os possíveis danos físicos e/ou materiais causados ao Órgão ou a terceiros, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança de Referência.

13. OBRIGAÇÕES DA CONTRATANTE

- 13.1. Todo o processo de instalação e implantação dos serviços será acompanhado e supervisionado pela Diretoria de Tecnologia da Informação e Comunicação da CONTRATANTE, à qual a CONTRATADA de cada lote deverá se reportar antes de qualquer ação e decisão referente à implantação da solução;
- 13.2. Fornecer informações e configurações necessárias para a configuração dos NGFWs fornecidos;
- 13.3. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 13.4. Viabilizar, por todos os meios ao seu alcance, para que a CONTRATADA possa prestar os serviços, fornecendo a qualquer tempo e com a máxima presteza, mediante solicitação por escrito da CONTRATADA, informações adicionais, dirimir dúvidas e orientá-la em todos os casos omissos;
- 13.5. Exercer o acompanhamento e a fiscalização do fornecimento e instalação, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;
- 13.6. Verificar se durante a vigência da contratação estão sendo mantidas todas as exigências, condições de habilitação e qualificação contratadas;



Câmara Municipal de Curitiba

- 13.7. Conferir, vistoriar e aprovar o fornecimento dos produtos entregues pela CONTRATADA;
- 13.8. Permitir o acesso dos empregados da CONTRATADA às dependências da Câmara Municipal de Curitiba, para o fornecimento dos itens e instalação de toda a solução necessária;
- 13.9. Atestar a efetiva prestação dos serviços, bem como a qualidade dos mesmos;
- 13.10. Avaliar a qualidade do serviço prestado pela Contratada, podendo rejeitá-lo no todo ou em parte, caso estejam em desacordo com as disposições deste Termo de Referência;
- 13.11. Notificar a CONTRATADA por escrito da ocorrência de eventuais falhas no fornecimento ou instalação, fixando prazo para a sua correção;
- 13.12. A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente objeto, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados;
- 13.13. Efetuar o pagamento pelo objeto, na forma convencionada no presente instrumento, desde que atendidas as formalidades previstas.

14. FATURAMENTO

- 14.1. A CONTRATADA deve fornecer fatura e notas fiscais pertinentes centralizadas com o mesmo CNPJ constante no contrato de prestação de serviços;
- 14.2. Para o caso de prestação de serviço realizada por filiais, a CONTRATADA deve informar os dados cadastrais, bem como CNPJ da mesma, no contrato de prestação de serviços discriminando o serviço a ser prestado pela filial em questão;
- 14.3. A CONTRATADA, se possuir sede fora do município de Curitiba, que emite notas fiscais para a CONTRATANTE nesta Capital, deve inscrever-se no Cadastro de Empresas Prestadoras de Serviços de Outros Municípios (CPOM);
- 14.4. O pagamento será efetuado através de ordem bancária, para crédito em banco, agência e conta-corrente indicados pela Contratada, no prazo de até 15 (quinze) dias consecutivos, contados da apresentação à Contratante da nota fiscal/fatura discriminativa contendo o detalhamento do produto e, se for o caso, dos materiais empregados, do número da Nota de Empenho, os números do Banco, da Agência e da conta-corrente da Contratada e a descrição clara e sucinta do objeto.
 - 14.4.1. Em casos excepcionais, a Contratada deverá permitir o pagamento das faturas mensais via boleto bancário.
- 14.5. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. Caso a Contratada seja regularmente optante pelo Simples Nacional não se procederá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.
- 14.6. A Contratante se reserva o direito de descontar o valor da(s) multa(s) aplicada(s) quando do pagamento da(s) fatura(s) emitida(s) pela(s) Contratada(s) e/ou proceder a execução direta do débito.
- 14.7. O pagamento está condicionado à apresentação, mediante envio da documentação para abertura do processo de pagamento diretamente ao fiscal e seu suplente, por meio de correspondência eletrônica ou outra forma convencionada entre as partes, mencionando os serviços e o valor a ser pago. Deverão ser sempre apresentadas:
 - 14.7.1. Nota Fiscal/Fatura (original), emitida em nome da Câmara;
 - 14.7.2. Fatura discriminativa (original)
- 14.8. A Contratada deverá apresentar ainda, sempre que solicitado pela Contratante, os documentos abaixo relacionados:
 - 14.8.1. Prova de regularidade para com a Fazenda Municipal da sede da empresa;

Página 36 de 37



Câmara Municipal de Curitiba

- 14.8.2. Prova de regularidade para com a Fazenda Estadual da sede da empresa;
- 14.8.3. Prova de regularidade conjunta, relativa a Tributos Federais e à Dívida Ativa da União;
- 14.8.4. Certificado de Regularidade do FGTS (CRF);
- 14.8.5. Prova de regularidade perante a Justiça do Trabalho (CNDT);
- 14.8.6. Extrato de Optante pelo Simples Nacional, se for o caso.
- 14.9. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras.
 - 14.9.1. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.
- 14.10. Na hipótese de irregularidade das certidões relacionadas nos itens 14.8.1, 14.8.2, 14.8.3, 14.8.4 ou 14.8.5, a Contratada deverá regularizar a sua situação no prazo de até 15 (quinze) dias, sob pena de aplicação das sanções administrativas e eventual rescisão da contratação.
- 14.11. Os pagamentos efetuados pelo Contratante não isentam a Contratada de suas obrigações e responsabilidades.
- 14.12. O pagamento somente será autorizado após a emissão de Atesto de Recebimento pelo servidor competente e verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos produtos efetivamente fornecidos e, eventualmente, aos materiais empregados.
- 14.13. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 14.14. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da fórmula:
$$I = (TX / 100) / 365$$
$$EM = I \times N \times VP, \text{ onde:}$$

I = Índice de atualização financeira;
 TX = Percentual da taxa de juros de mora anual;
 EM = Encargos moratórios;
 N = No de dias entre a data prevista para pagamento e a do efetivo pagamento;
 VP = Valor da parcela em atraso.

Curitiba, 16 de fevereiro de 2023.

DÉBORA REIS LEAL DE LIMA

Setor de Planejamento e Desenvolvimento de
Projetos

TARCÍSIO SOCHER

Diretoria de Tecnologia da Informação
e Comunicação

BRUNO SILVA DE OLIVEIRA

Divisão de Arquitetura de Serviços - Diretoria de
Tecnologia da Informação e Comunicação -
DTIC