Memorando n° 119/2023/SITI/SMSA

Santa Maria, 18 dezembro de 2023.

De: Secretaria de Município de Inovação e Tecnologia da Informação

Para: **Secretaria de Município de Finanças**
**Superintendente de Compras e Licitações**

Assunto: **Resposta impugnação PE 170/2023.**

Cuida-se de resposta ao Recurso Administrativo, recebido de DAISON LAURENCE WOBETO relativo ao Pregão Eletrônico nº 170/2023, o qual passamos a responder:

**a) objeto do contrato utilizado como justificativa não guarda correlação com o objeto licitado neste Edital**

**b) pelo evidente direcionamento de marca, amparado em justificativa desprovida de documentação técnica adequada**

Considerando que a Administração Pública está vinculada aos princípios da eficiência e da economicidade. A Constituição da República de 1988 (CRF/1988) determinou como regra a obrigatoriedade do processo licitatório para toda administração pública, direta, indireta e fundacional nos termos do seu artigo 37, inciso XXI, visando alcançar a proposta mais vantajosa financeiramente e tecnicamente para os interesses da administração no âmbito de suas contratações. Nesse sentido, destacam-se os referidos princípios no que se refere às licitações e aos contratos formalizados pela administração pública. Isso porque tais princípios zelam, respectivamente, por aperfeiçoar a alocação dos recursos públicos nas contratações e por alcançar a alternativa mais vantajosa do ponto de vista econômico.

Dito isto, quanto ao questionamento temos a discorrer que a definição clara e precisa do objeto é indispensável ao bom andamento do certame. Assim, necessário se faz uma adequada caracterização do objeto a ser licitado, com especificações técnicas claras, objetivas e estritamente vinculadas à necessidade apontada para que a licitação venha a ser bem sucedida.

Conforme evidencia Marçal Justen Filho, no Livro Comentários à Lei de Licitações e Contratos Administrativos, 15ª Edição, o princípio da padronização constitui regra a ser seguida pela Administração, que deverá ter em vista produtos semelhantes que já integram o patrimônio público, como também deverá prever eventuais futuras aquisições. Somente assim a padronização produzirá os efeitos desejados. Ademais, para o Jurista, consagra-se a padronização como instrumento de racionalização administrativa, com redução de custos e otimização da aplicação de recursos. Significa que a padronização elimina variações no tocante à seleção de produtos no momento da contratação como também na sua utilização, etc. Segundo Gasparini, a padronização é a regra, sendo necessário que a impossibilidade da aquisição de certos bens, com a observância desse princípio, fique devidamente demonstrada, senão restaria inócuo e não teria qualquer utilidade a determinação “sempre que possível”, consignada no caput do art. 15.

O elevado grau de criticidade dos processos conduzidos pelo Município de Santa Maria a confiar e depender cada vez mais de sua infraestrutura tecnológica para viabilizar aplicações e implementar rapidamente novas soluções que aumentem a agilidade, a capacidade de adaptação, a otimização de custos e a melhoria dos serviços prestados, de forma continuada, aos cidadãos.

Atender essa demanda garantindo alta qualidade e eficiência, confiabilidade, flexibilidade e agilidade, é preocupação constante da administração, o que tornou a área de tecnologia da informação uma ferramenta estratégica que deve estar alinhada com todos as secretarias municipais.

Diante deste cenário, as informações disponibilizadas nesses serviços tornaram-se alvo de criminosos cibernéticos. Houve crescimento exponencial de ataques cibernéticos altamente agressivos especialmente a partir de 2020. Ataques cibernéticos foram responsáveis pelas paralisações das atividades em diversos setores do país, incluindo o Município de Santa Maria, cujo ataque através de *ransonware*[1] ocorrido em 2023 gerou indisponibilidade dos serviços, devido à escassez de profissionais de segurança de informação e ferramentas forenses de TI, impediu a rápida resposta ao incidente. Ademais, sem tais recursos, é impossível afirmar que o atacante deixou o ambiente, havendo a possibilidade de ter malwares ou backdoors[2] instalados no ambiente de TI, facilitando consideravelmente um novo ataque.

1Tipo de malware que criptografa o sistema de arquivos do equipamento infectado e o atacante solicita um valor financeiro para descriptografar os dados.

2Um backdoor em um software ou sistema de computador é geralmente uma porta de acesso não documentada que permite ao atacante entrar nos sistemas corporativos furtivamente.

Portanto, devido à criticidade da disponibilidade dos serviços e preservação da integridade dos dados dos cidadãos, são necessárias ações preparatórias (proativas) e de remediação (serviços especializados) que tenha como objetivo a conformidade com as melhores práticas em prevenção, gerenciamento e investigação de ataques cibernéticos, sempre com o objetivo maior de tentar evitar ou mitigar os possíveis danos que tais ataques são capazes de produzir.

O Município de Santa Maria vem investido constantemente em soluções que reforcem a proteção contra-ataques cibernéticos, sejam eles internos ou externos, ao ambiente. Em 2019 foi adquirido, através do contrato 486/2022, solução de Firewall de Próxima Geração, do fabricante Fortinet, com o objetivo de proteger a rede interna de ameaças externas.

Não obstante, uma solução de firewall é essencial para as organizações por diversos motivos, sendo a segurança de rede um dos principais. Um firewall é um componente de segurança que atua como uma barreira entre a rede interna de uma organização (como computadores, servidores, dispositivos) e a Internet ou outras redes externas. Entre as diversas funções realizadas por esta solução, podem ser citadas: Proteção contra ameaças externas:

- Um firewall ajuda a impedir que ameaças externas, como hackers, malware, vírus e ataques cibernéticos, acessem a rede interna da organização. Ele filtra o tráfego de entrada e saída, garantindo que apenas o tráfego autorizado e seguro passe pelo sistema.
- Controle de acesso: O firewall permite que a organização controle quais serviços, aplicativos ou portas de rede podem ser acessados pelos usuários internos e externos. Isso evita o acesso não autorizado a recursos sensíveis e ajuda a manter a privacidade dos dados.
- Monitoramento de tráfego: Um firewall registra informações detalhadas sobre o tráfego de rede, permitindo que a equipe de segurança acompanhe as atividades e detecte potenciais comportamentos suspeitos ou intrusões.
- Segurança de aplicações: Além de proteger a rede, alguns firewalls também fornecem recursos de proteção para aplicativos específicos, como filtragem de URL, prevenção de intrusões (IPS), proteção contra ataques de negação de serviço (DoS), entre outros.
- Cumprimento de normas e regulamentos: Em muitos setores, as organizações são obrigadas a seguir normas e regulamentos de segurança cibernética. Um firewall pode ser uma parte importante desses requisitos de conformidade.

- Segmentação de rede: Por meio do uso de firewalls internos, as organizações podem segmentar sua rede em zonas de segurança separadas, criando camadas adicionais de proteção. Isso limita o alcance de possíveis violações e impede que um único ponto de falha comprometa toda a rede.
- Continuidade dos negócios: Ao evitar ameaças cibernéticas e ataques, o firewall ajuda a garantir a continuidade das operações da organização, minimizando o impacto de possíveis interrupções.

Dessa forma, uma solução de firewall é uma parte crucial da estratégia de segurança cibernética de qualquer organização, protegendo seus ativos digitais, dados sensíveis, infraestrutura e, em última instância, sua reputação. É importante que a equipe de segurança da organização mantenha o firewall atualizado e configure-o adequadamente para atender às necessidades específicas da empresa e às ameaças emergentes no cenário de segurança cibernética.

Contudo, a solução de firewall, apesar da sua eficácia na proteção do perímetro de rede, não é capaz de proteger todos os vetores possíveis de ataque, tais como:

- Usuário com dispositivo removível infectado (exemplo: pen drive);
- Arquivos e links maliciosos encaminhados através de e-mail;
- Malwares já instalados na rede que podem se movimentar lateralmente, ou seja, de uma máquina a outra pela rede interna, sem passar pela inspeção do firewall;
- Roubo de credenciais, sendo que, neste caso, para as soluções de segurança, o acesso é tratado como legítimo;
- Usuário interno mal-intencionado.

De acordo com a consultoria de soluções de tecnologia Gartner, a melhor abordagem para proteger o ambiente de tecnologia, principalmente considerando funcionários remotos, é através de uma arquitetura chamada CSMA (Cyber Security Mesh Architecture). No modelo anterior, implementado em boa parte dos ambientes de TI, temos diversos fabricantes, sem integração entre si, e com pouca visibilidade holística do ambiente, dificultado a identificação do ataque e gerando custo mais elevados de administração.

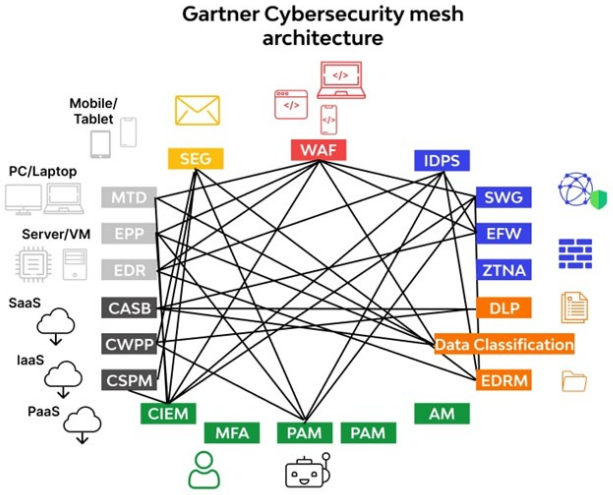


*Figura 1: Gartner CSMA*

No modelo CSMA, conforme figura 1, há integração entre as mais diferentes ferramentas, permitindo a correlação dos eventos, bloqueio mais rápido das ameaças e um menor tempo de identificação da ameaça (MTTD) e menor tempo para resolução (MTTR).

Há uma grande variedade de fabricantes de soluções de segurança. Entretanto, é importante reforçar que há muita complexidade na administração e gerenciamento destas ferramentas, e a integração entre elas não é a melhor abordagem de acordo com o Gartner.

Atualmente estão implementados os equipamentos do fabricante *Fortinet*, e esta equipe técnica considera que se deve manter tal fabricante, que inclusive ainda está com o contrato de suporte ativo. Portanto, a melhor estratégia é defender os outros vetores de ataque através da contratação de uma solução do mesmo fabricante, permitindo a utilização da abordagem proposta pelo Gartner, além de:

- Curva de aprendizado: Cada fabricante possui sua própria interface de gerenciamento, terminologia, configurações e recursos específicos. Ao trocar de fabricante, a equipe de TI e segurança precisará se adaptar a uma nova plataforma e aprender a trabalhar com ela. Isso pode exigir treinamento adicional e tempo para se familiarizar com a nova solução.
- Integração com o ambiente existente: A migração para uma nova solução de firewall é complexa especialmente em organizações que já possuem uma infraestrutura implantada e vários sistemas interligados. A integração da nova solução com o ambiente existente pode requerer esforço significativo e cuidadosa coordenação para garantir que todos os serviços e aplicativos continuem funcionando sem problemas.

- Perda de configurações personalizadas: As configurações e regras personalizadas feitas na solução anterior podem não ser diretamente transferíveis para a nova plataforma, como configurações de alta disponibilidade de links de Internet, *Internet Database Services*, inspeção de tráfego de dados em profundidade (*deep inspection*). Isso significa que a equipe de segurança precisará recriar todas as configurações personalizadas na nova solução, o que pode ser um processo demorado e propenso a erros, e exigir complementações com outras soluções para que seja possível obter o mesmo resultado.
- Possíveis interrupções de serviço: Durante o processo de migração, pode haver interrupções temporárias nos serviços de rede e comunicação. Se a transição não for bem planejada e executada, isso pode levar a períodos de indisponibilidade não planejados, o que pode afetar negativamente as operações da organização.
- Risco de inconsistências de segurança: muitos fabricantes e soluções diferentes podem criar brechas de segurança temporárias e até definitivas se as regras e configurações não forem adequadamente integradas na nova. Isso pode deixar a rede vulnerável a ataques ou ameaças durante o período de transição.

Desta forma, esta equipe técnica propõe uma contratação de TI de acordo com os princípios de efetividade, economicidade, qualidade, segurança, transparência e legalidade. Tendo como princípios técnicos:

- Manter a padronização do ambiente de proteção e segurança cibernética, que atualmente utiliza fabricante *Fortinet*;
- Eliminar os principais pontos únicos de falha, tornando a rede mais robusta e reduzindo o impacto causado por possíveis falhas;
- Maximizar o retorno sobre os investimentos realizados;
- Atender inclusive sistemas operacionais legados, ainda em uso na infraestrutura do Município.

A solução proposta foi escolhida para garantir a preservação deste investimento, pois trata-se de equipamentos no mesmo padrão dos já instalados, o que potencializa a utilização dos atuais por todo o tempo de vida de cada dispositivo. Além do fator econômico, é importante destacar que a solução proposta facilitará a interoperabilidade entre os componentes, o gerenciamento centralizado, a economia de escala e o aproveitamento do conhecimento da equipe técnica.

Não há nenhum tipo de cerceamento da competitividade na definição do fabricante Fortinet para a garantia do melhor interesse do Município de Santa Maria e para a lisura e

competitividade de um procedimento licitatório idôneo, uma vez que existem diversos representantes autorizados pela fabricante para oferecerem os equipamentos solicitados.

Portanto, para elevar o nível de segurança e tratar o incidente de segurança ocorrido, as seguintes soluções são necessárias:

- **Managed Endpoint Detection and Response (EDR com MDR):** Este tipo de solução complementa o antivírus tradicional que é baseado apenas em assinaturas, permitindo a análise comportamental e de indicados de comprometimento (IoC) fornecidos pelos fabricantes ou gerados internamente. O EDR pode reduzir drasticamente o MTTD e MTTR uma vez que é capaz de bloquear o ataque, mas também é capaz de prover a resposta ao incidente e triagem de eventos relacionados as estações de trabalho. Mas somente a ferramenta não é suficiente. Devido a falta de efetivo, é crucial que esta ferramenta seja monitorada pelo fabricante, que deve, minimamente, informa a prefeitura equipamentos comprometidos, tipo de ataque ocorrido e possíveis passos para mitigação. Este serviço provido pelo fabricante que gerencia o EDR é conhecido como MDR e deve ser integrado a solução de firewall Fortinet existente, permitindo, por exemplo, o bloqueio de um endereço IP.
- **Solução de Zero Trust com antivírus tradicional (ZTNA):** A solução de ZTNA baseia-se no conceito de zero-trust, ou confiança zero, permitindo que apenas os usuários / grupos corretos, acessem determinadas aplicações e recursos da rede. No modelo tradicional de VPN, o usuário tem acesso a diversos recursos internos, o que ocasiona o aumento da superfície de ataque. Portanto, uma solução de ZTNA garante que apenas os recursos que ele precisa estarão acessíveis e todo os demais negado e bloqueados através da integração da solução de endpoint com o firewall de próxima geração Fortinet existente. Ademais, esta solução de ZTNA deve incluir a proteção do antivírus tradicional (EPP), com assinaturas atualizadas no mínimo diariamente, sendo esta uma ferramenta básica de segurança em qualquer ambiente de TI. Para aumentar o nível de segurança, a solução de EPP deve incluir proteção contra ransonware, inteligência artificial para detecção de malwares e controle de dispositivo removível, tal como pen drive.
- **Múltiplo fator de autenticação (MFA):** O problema de roubo de credenciais é grave um dos mais comuns, pois, envolve principalmente o comportamento humano no processo. Portanto, um usuário descuidado pode acabar tendo suas credenciais comprometidas e posteriormente utilizadas para um ataque. A maneira mais eficaz na proteção deste tipo de situação é através da implementação de uma solução de MFA. Portanto, ainda que o atacante possua as credenciais, ele não

terá acesso ao token gerado automaticamente a cada 30 segundos e terá seu acesso negado. A solução deve ser composta por um servidor de autenticação e tokens para instalação em dispositivos móveis, tais como: Apple IOS e Android.

- **Solução de análise de logs avançada:** Para elevar o nível de segurança, é necessária uma solução que concentre os logs gerados tanto pelas soluções de endpoint, quanto para a solução de firewall. Mas somente armazenar os logs não é suficiente. A solução também deve ser capaz de gerar relatórios de tráfego e de incidentes, bem como haver um serviço do fabricante para deteção de IoCs (gerados pelo fabricante) nos logs armazenados e um serviço de alerta e detecção para campanhas de malwares que estão se alastrando mundialmente. É importante que a solução também seja capaz de armazenar os logs para pesquisas forenses, avaliações futuras e “threat hunting” pelo período mínimo de 12 (doze meses).
- **Serviço de investigação forense:** com o intuito de investigar o ambiente existente, identificou-se a necessidade de contratação de um serviço de análise forense para avaliar as condições do ambiente existente. O objetivo é identificar se o atacante ainda tem acesso ao ambiente, efetuar a correção da falha e implementar as novas ferramentas.
  - Avaliação de comprometimento e riscos;
  - Apoio na definição do processo de resposta ao incidente;
  - Serviço de “threat huting”;
  - SLA inferior a 4 horas para tratamento de incidentes;
  - O serviço deve ser executado em até 12 meses.

A impugnante ignora a premissa de quem delimita as necessidades técnicas de uma contratação é a área técnica, ao afirmar direcionamento desta contratação, uma vez que quando se delimita as necessidades técnicas mínimas, são tomadas por base diversos fornecedores, que realizaram sugestões e cotações de novas tecnologias para tratar o incidente de segurança em questão. Incidente este que destacou o ponto fraco da infraestrutura do município como sendo a solução de antivírus do modelo antigo, dependente de atualizações e do reconhecimento de assinaturas de vírus para se defender.

Portanto, ao contrário do que sustenta o impugnante, está devidamente demonstrada a necessidade de manter a padronização do ambiente de proteção e segurança cibernética, que atualmente utiliza fabricante Fortinet. Assim, a exceção da

vedação constante do §5º art. 7º da Lei 8.666, de 1993, o órgão solicitante justificou tecnicamente a exigência do equipamento e, ainda, acima de tudo, demostrou a economicidade da contratação que ora se busca perfectibilizar.

## CONSIDERAÇÕES FINAIS

Ante ao exposto, determinamos **improcedente** o recurso demandado por Daison Laurence Wobeto.

Atenciosamente,

TIAGO MARTINI SANCHOTENE:01848367007

Assinado digitalmente por TIAGO MARTINI SANCHOTENE:01848367007
DN: C=BR, O=ICP-Brasil, OU=Secretaria da Receita Federal do Brasil - RFB, OU=RFB e-CPF A1, OU=(EM BRANCO), OU=22180785000164, OU=videoconferencia, CN=TIAGO MARTINI SANCHOTENE:01848367007
Razão: Eu estou aprovando este documento
Localização: sua localização de assinatura aqui
Data: 2023-12-18 10:36:42
Foxit Reader Versão: 10.0.1

**TIAGO MARTINI SANCHOTENE**
Secretário de Município de Inovação e Tecnologia da Informação

ASSINADO DIGITALMENTE
SABRINA MEDIANEIRA DA SILVA AVILA
A conformidade com a assinatura pode ser verificada em: http://serpro.gov.br/assinador-digital
SERPRO

**SABRINA MEDIANEIRA DA SILVA AVILA**
Analista de Sistemas