CÂMARA MUNICIPAL DE GOIÂNIA | ESTADO DE GOIÁS PODER LEGISLATIVO

ESTUDO TÉCNICO PRELIMINAR (ETP)

Setor Requisitante:	**Diretoria de Tecnologia da Informação**
Processo Eletrônico:	**00000.004492.2024-98**

1. INFORMAÇÕES GERAIS

O presente documento caracteriza a primeira etapa da fase de planejamento e apresenta os devidos estudos para a contratação de solução que atenderá à necessidade abaixo especificada.

O objetivo principal é estudar detalhadamente a necessidade e identificar no mercado a melhor solução para supri-la, em observância às normas vigentes e aos princípios que regem a Administração Pública, nos moldes da Lei Federal nº 14.133/2021 e da Portaria nº 454, de 15/03/2023, da Câmara Municipal de Goiânia.

2. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL (PCA)

Previsto no PCA do ano de 2025 através do DFD 12/2024 - DRTIN.

3. DESCRIÇÃO DA NECESSIDADE

A CMG possui um parque computacional para atendimento aos usuários, com cerca de 400 computadores ativos na rede.

É essencial garantir a proteção e a integridade dos dados e sistemas da

CMG, bem como a segurança dos usuários e da informação compartilhada. Portanto, é necessário implementar medidas de monitoramento contínuo, análise de logs, detecção de anomalias e resposta rápida a incidentes, a fim de mitigar riscos e garantir um ambiente seguro e confiável para as operações da CMG.

É crucial fornecer à CMG recursos de segurança atualizados, capazes de monitorar e responder a infecções causadas por software malicioso desenvolvido por indivíduos com más intenções. Esses recursos abrangem desde a exposição simples de informações obtidas até a exigência de pagamento de resgate para a liberação de dados sequestrados, como ocorre nos ataques de ransomware. Além disso, é essencial que esses recursos garantam a detecção proativa de ameaças, a implementação de medidas preventivas, a resposta rápida a incidentes e a recuperação eficiente dos sistemas afetados.

O objetivo em questão visa minimizar a vulnerabilidade dos sistemas corporativos, redes, estações de trabalho, caixas postais, implementando metodologias de segurança de antivírus corporativo, prevenindo possíveis ataques internos e externos de vírus, spams e spywares e outras ameaças virtuais ao ambiente tecnológico da CMG.

A contratação visa estabelecer práticas de segurança cibernética sólidas, alinhadas com as melhores práticas e padrões do setor. Esse enfoque na segurança cibernética é essencial para mitigar riscos e proteger a integridade dos dados da CMG, sendo fundamental para garantir um ambiente seguro e confiável para a manipulação e proteção dos dados pessoais, cumprindo as exigências legais e fortalecendo a postura de segurança da CMG.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Solução de proteção avançada contra ataques cibernéticos para estações de trabalho;
4.2. A solução deverá ser entregue na modalidade como um serviço (em nuvem);
4.3. Possuir console Web para gerenciamento e administração da ferramenta;
4.4. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente;
4.5. Módulo de Proteção Anti-Malware;
4.6. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.6.1. Windows 7;
4.6.2. Windows 10;
4.6.3. Windows 11.

4.7. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;
4.8. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM);
4.9. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
4.10. Deve possuir detecção heurística de vírus desconhecidos;
4.11. Funcionalidade de Atualização
4.12. Funcionalidade de Administração
4.13. Funcionalidade de Controle de Dispositivos
4.14. Funcionalidade de HIPS – Host IPS e Host Firewall
4.15. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;
4.16. Módulo para Controle De Aplicações
4.17. Módulo de Detecção e Resposta
4.18. Deve disponibilizar suporte ao usuário

4.18.1. Disponibilizar os seguintes canais de acesso ao suporte técnico:

- Portal Web;
- E-mail;
- Central 0800; e/ou
- Telefone fixo.

4.18.2. O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso

4.19. Deve disponibilizar serviço de implantação
4.20. Deve disponibilizar serviço de treinamento

5. ESTIMATIVA DAS QUANTIDADES

Levando em consideração o quantitativo atual de cerca de 400 estações de trabalho, será suficiente aquisição de 450 licenças da solução de proteção.

O valor de 450 licenças é o suficiente para garantir demanda futura por 3 anos(período de vigência das licenças), visto que existe previsão de concurso (em torno de 50 servidores) sendo necessários em torno 25 computadores para absorver esses servidores. Existirá também o aumento de gabinetes de vereadores (5 gabinetes novos). Sendo assim para cada gabinete, tem-se 4 computadores, totalizando 20 computadores para novos gabinetes.

Somando os 25 computadores do concurso com os 20 computadores dos gabinetes tem-se um total de 45 computadores adicionais. Conclui-se que esse quantitativo adicional está contemplado nas 450 licenças que se pretende adquirir.

6. LEVANTAMENTO DE MERCADO

Foram verificadas 3 soluções:

- Antivírus Tradicional
- Antivírus + EDR (Endpoint Detection and Response)
- Antivírus + EDR + XDR (Extended Detection and Response)

A solução de antivírus tradicional atende a maioria dos casos conhecidos de vírus, tem o custo mais baixo, é de fácil implementação. No entanto, é ineficaz a ameaças novas e desconhecidas, não fornece informações detalhadas sobre incidentes, e não é eficiente contra ataques sofisticados.

A solução de Antivírus + EDR ja é atualmente utilizada pela CMG. Ela detecta proativamente, isola computadores comprometidos, investiga incidentes em profundidade e responde rapidamente a ataques, além de ter uma visão centralizada dos ataques. No entanto, tem um custo mais alto, requer um conhecimento técnico, e exige mais recursos computacionais.

A solução de Antivírus + EDR + XDR integra dados de computadores, redes, e-mails e outras fontes, proporcionando uma visão ampla dos ataque e facilitando a correlação de eventos, oferece uma detecção mais aprimorada e respostas coordenadas, proporciona análises mais completas e eficientes, reduzindo o tempo necessário para investigar e mitigar ameaças em toda a infraestrutura. No entanto, tem uma maior complexidade de implementação e gestão, com custo também significativamente maior.

Para a aquisição da opção mais avançada - o XDR - seria necessário uma equipe bem definida de segurança de rede, pois neste esquema deve-se observar os eventos que acontecem na rede diariamente. Caso essa equipe não exista, o recurso do XDR ficaria sem utilização eficaz. Hoje não temos mão de obra suficiente para fazer esse tipo de composição.

Descarta-se a opção do antivírus tradicional visto que ele oferece um nível de segurança menor que a solução atualmente utilizada (antivírus + EDR), não atingindo o objetivo de proteger da melhor forma os computadores com melhor custo benefício.

Conclusão, o antivírus + EDR é o ideal para ser adquirido, levando-se em consideração que há a necessidade de respostas rápidas, nossa infraestrutura é relativamente simples, e possui um custo muito menor que o XDR. Opta-se pela solução intermediária: Antivírus + EDR.

7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Justificativa para o sigilo do valor estimado: A opção pelo orçamento sigiloso se justifica em virtude da busca pela maior vantajosidade da proposta, garantindo a ampla competitividade e economicidade para a Administração, a fim de obter o preço compatível com o praticado no mercado.

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução faz a proteção dos computadores da CMG contra ataques cibernéticos, atuando no nível mais critico a ser protegido, é um ponto fraco onde a maioria dos ataques acontece ou se inicia.

Além das funcionalidades tradicionais de antivírus, será contratada a funcionalidade de EDR (Endpoint Detection and Response). Esta fará a avaliação de onde começou o ataque, que tipo de ataque se trata, quais ações o ataque tentou fazer no sistema. Assim pode-se isolar a máquina e ter uma visualização centralizada de onde estão acontecendo os ataques, programada também ações automática para cada caso.

As licenças são aplicadas por computador e duram 3 anos (36 meses).

9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

Trata-se de um único objeto indivisível.

10. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS (BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO)

Continuar aplicando o mesmo nível de segurança atual, aplicando a solução de antivírus + EDR a fim de manter protegido todo o parque computacional da CMG.

11. ANÁLISE DOS RISCOS ASSOCIADOS À DEMANDA

11.1. Dos riscos associados ao planejamento da contratação:

Para a presente contratação, identifica-se alguns riscos que poderão ocorrer na fase de planejamento: falha na elaboração do TR (especificação imprecisa do objeto); atraso no processo administrativo de contratação; pesquisas de mercado mal avaliadas; falta de experiência da Administração na contratação pretendida; valor estimado da contratação acima do valor previsto no orçamento; falha no método utilizado para realizar a estimativa de preços; requisitos de habilitação exigidos no edital de forma desproporcional; dentre outros.

Todos os riscos identificados podem prejudicar a contratação e não atender as necessidades da Câmara, de forma a ocorrer: arquivamento do processo licitatório; impugnação de edital; contratação de valores superfaturados em violação ao princípio da economicidade; restrições às condições de participação do certame em ofensa ao princípio da isonomia e competitividade e ineficiência na prestação do serviço ou na entrega dos produtos.

Para uma contratação eficiente, necessário se faz que todos os envolvidos nesta fase de planejamento elaborem os documentos com definições claras, detalhadas e realizem os procedimentos necessários com critérios objetivos e impessoais, primando sempre pela moralidade administrativa e pelo interesse público.

11.2. Dos riscos associados à seleção do fornecedor:

Na fase de seleção do fornecedor, foram identificados alguns riscos

como: possibilidade de ocorrer uma licitação fracassada ou deserta; atraso ou suspensão no processo licitatório em face de impugnações ou recursos; valores de alguns itens licitados superiores aos estimados (sobrepreço) e outros com subpreço, sendo o menor valor global proposto; contratação de fornecedor com baixa qualificação técnica; empresas sem qualificação econômico-financeira adequada.

A ocorrência desses riscos pode resultar no arquivamento do processo licitatório; na contratação de empresa incapaz de executar o serviço ou fornecer os produtos ou incapaz de executar o objeto de forma satisfatória, bem como pode ocorrer o não cumprimento de obrigações financeiras, trabalhistas e fiscais. Tais situações podem gerar extinção contratual e dano ao erário, comprometendo o resultado esperado, além de prejudicar as atividades desenvolvidas na Câmara.

11.3. Dos riscos associados à gestão contratual:

Os riscos identificados na fase de execução desta contratação são: falta de ferramenta própria para uma boa gestão; baixa qualificação técnica dos profissionais da empresa para execução do contrato; elementos básicos do contrato não estarem claros para as partes; atraso na prestação dos serviços ou fornecimento dos produtos; inadimplemento de obrigações contratuais e alterações das condições econômico-financeiras da contratada.

A ocorrência dos riscos identificados pode gerar o comprometimento dos serviços prestados ou dos produtos fornecidos, descontinuidade contratual, necessidade de contratação emergencial, paralisação temporária de atividades da Câmara, dentre outros.

12. PROVIDÊNCIAS PRÉVIAS À CELEBRAÇÃO DO CONTRATO

Não serão necessárias providências prévias à celebração do contrato.

13. CONTRATAÇÕES CORRELATAS E INTERDEPENDENTES

Não se aplica.

14. POSSÍVEIS IMPACTOS AMBIENTAIS

Por se tratar de objeto imaterial (programa de computador), não foram observados impactos ambientais relevantes além do uso adicional de recursos computacionais de cada máquina consumindo uma quantidade maior de energia elétrica.

15. VIABILIDADE DA CONTRATAÇÃO

Conclui-se que a contratação é necessária para a continuidade da segurança nas estações de trabalho, equipamentos do DATACENTER e dos sistemas informatizados da CMG.

Pedro Henrique Rodrigues Pinheiro
Responsável pela Elaboração do ETP
Local, 18 de novembro de 2024

De acordo:

Maycon Dias de Lima

Diretor do Setor Requisitante