ESTUDO TÉCNICO PRELIMINAR

PROCESSO ADMINISTRATIVO ELETRÔNICO Nº 3550/2024

(Contratação de Pessoa Jurídica especializada na prestação de serviços de solução integrada de Cibersegurança)

Fevereiro de 2025

ESTUDO TÉCNICO PRELIMINAR - ETP

1. INTRODUÇÃO

Estudo Técnico Preliminar (ETP) consiste no instrumento inicial da fase preparatória da licitação, no qual se expõem o interesse público e a melhor solução sob os aspectos mercadológico, técnico, ambiental, cultural e econômico da contratação, com o objetivo de indicar a viabilidade da contratação e servir de base para edição do Termo de Referência ou Projeto Básico.

O ETP indicará os problemas a serem resolvidos e concluirá pela melhor solução evidenciada, considerando a gestão, os riscos e os aspectos mercadológico, técnico, ambiental, cultural e econômico da contratação.

Este instrumento terá o objetivo de identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Formalização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referente ao Processo Administrativo eletrônico nº 3550/2024.
Setor Requisitante: DIVISÃO DE INFORMÁTICA
Responsável pela Demanda: Ricardo Williams Paixão Ferraz
Área Técnica: DIVISÃO DE INFORMÁTICA
Data: 07/02/2025
Fundamentação jurídica: art. 18, §2º, da Lei Federal nº 14.133/2021 e Resolução nº 580 de 2023 CMR.

2. DESCRIÇÃO DA NECESSIDADE

2.1. IDENTIFICAÇÃO DA NECESSIDADE E DOS PROBLEMAS

Contratação de empresa especializada para a prestação de serviços de segurança cibernética para a Câmara Municipal do Recife. Esta contratação visa oferecer condições para se garantir a disponibilidade, confidencialidade, sigilo e a continuidade dos serviços e programas institucionais sustentados pelo ambiente de Tecnologia da Informação e Comunicação (TIC) da CÂMARA MUNICIPAL DO RECIFE, sendo necessário:

- Gerar relatórios que permitam garantir a efetividade de controles de segurança, assim como uma visão do estado atual e histórico de ocorrências;
- Analisar o ambiente, coletando informações e evidências de suspeitas de ataques possibilitando o tratamento e a tomada de decisão em caso de identificação de ataques;
- Permitir a identificação de tentativas ou acessos, aceitos ou rejeitados, ao ambiente computacional da CÂMARA MUNICIPAL DO RECIFE;
- Implantar níveis de segurança alinhados aos padrões ISO-27001, ISO-27002, ISO-27005, ISO-27011 e ISO 27014;
- Monitoramento completo dos eventos de segurança dos ativos de informação;
- Manutenção de análise histórica dos eventos de segurança, coletando e correlacionando os eventos;
- Detectar atividades não autorizadas de processamento de informações;
- Dispor de meios para operação, administração e atendimento de requisições relacionadas às ferramentas e soluções de segurança disponíveis no ambiente tecnológico da CÂMARA MUNICIPAL DO RECIFE;
- Dispor de meios para identificação e correção de vulnerabilidades de segurança da informação no ambiente e sistemas críticos da CÂMARA MUNICIPAL DO RECIFE a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas;
- Operacionalizar a Gestão de Riscos de Segurança da Informação;
- Facilitar a identificação preventiva de ameaças emergentes ou invasões externas além de prevenir eventuais vazamentos de informações antes da divulgação pública;
- Implantar processo estruturado e instrumentalizado de gerenciamento de incidentes de segurança da informação, em que as etapas de triagem, classificação, análise, resposta e comunicação sigam as melhores práticas internacionais;
- Redução dos riscos de interrupção dos serviços e sistemas em decorrência de ataques cibernéticos;
- Criar bases históricas e estatísticas de incidentes, permitindo traçar tendências ou pontos que necessitam de aprimoramento;
- Responder mais rapidamente aos ataques cibernéticos;
- Desenvolver resiliência e melhorar a capacidade da TI de enfrentar eventos adversos relacionados a cibersegurança;

- Investir no desenvolvimento de processos de trabalho seguros, ao invés de apenas investir em tecnologia;
- Definição clara dos objetivos, produtos, prazos, custos, padrões de qualidade, responsabilidades das partes, além de indicadores de desempenho; e
- Melhoria da percepção do adequado gerenciamento de segurança de Segurança da Informação por parte da alta administração e dos usuários internos e externos, deixando transparente que há efetivo gerenciamento dos incidentes de segurança de tecnologia da informação.

2.2. IDENTIFICAÇÃO DAS NECESSIDADES TÉCNICAS

Visto que, no quadro funcional da CMR, ainda não há servidores especializados e qualificados para a prestação dos serviços em questão, torna-se necessária a imediata alocação dos serviços demandados. Essa alocação é essencial para garantir o bom andamento dos serviços da CÂMARA MUNICIPAL DO RECIFE.

Em caso de incidentes, a falta desses serviços pode acarretar graves consequências para toda a infraestrutura de informática que depende deles, resultando em falhas catastróficas nos equipamentos do datacenter.

Essas falhas causariam perdas físicas e paralisariam parte essencial dos serviços prestados à sociedade, colocando em risco tanto as atividades meio quanto as atividades finalísticas da CÂMARA MUNICIPAL DO RECIFE.

Diante dessa situação, fica evidente a urgência na contratação e o alto risco de danos e prejuízos caso a contratação não seja bem-sucedida.

2.3. IDENTIFICAÇÃO DA NECESSIDADE COMO CONTÍNUA OU TEMPORÁRIA

A necessidade é contínua, pois a proteção dos dados e a segurança cibernética exigem manutenção e atualização constante para acompanhar a evolução tecnológica e as novas ameaça.

2.4. IDENTIFICAÇÃO DE OUTROS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO

Os requisitos a que a solução contratada deverá atender incluem:

- Facilidade de instalação e configuração da solução, incluindo customização conforme as necessidades específicas da Câmara.
- Treinamento oficial para a equipe técnica, garantindo a operação eficaz do sistema.
- Operação assistida para suporte contínuo e resolução de incidentes.

- Alta disponibilidade e confiabilidade, com mecanismos robustos de backup e recuperação de dados.
- Conformidade legal com a Lei Geral de Proteção de Dados e outras normativas aplicáveis.

3. PREVISÃO NO PLANO DE CONTRATAÇÃO ANUAL

3.1. A Câmara Municipal do Recife ainda não elabora o Plano de Contratações Anual, dada a facultatividade trazida pela Lei nº 14.133/21, em seu art. 12, VII, em que o legislador utilizou o verbo 'poderá', ao se referir à elaboração do PCA pelos entes públicos.

3.2. Mesmo assim, a demanda se encontra em alinhamento com as diretrizes de gestão da entidade, além de ter alinhamento com as peças orçamentárias, como será demonstrado da indicação da dotação orçamentária devida.

4. REQUISITOS DA CONTRATAÇÃO

É esperado da solução de cibersegurança:

- Capacidade de escalabilidade da solução para atender a futuras expansões e necessidades de proteção adicional.
- Compatibilidade com infraestruturas e sistemas já existentes na Câmara Municipal do Recife.
- Facilidade de integração com outras ferramentas e soluções de segurança.
- Garantia e suporte técnico contínuo, com serviços de atualização e manutenção para atender às necessidades e requisitos da CÂMARA MUNICIPAL DO RECIFE.

Gestão de Vulnerabilidades, o objetivo desse serviço é identificar as possíveis vulnerabilidades de segurança da informação no ambiente da CÂMARA MUNICIPAL DO RECIFE (infraestrutura e aplicações), que seriam vetores de ataques e fixar uma blindagem contra a exploração dessas vulnerabilidades, evitando que ataques cibernéticos obtenham sucesso. Espera-se da CONTRATADA as orientações, o acompanhamento e a verificação das aplicações das correções de vulnerabilidade.

Gestão de Segurança para Infraestrutura e Sistemas Críticos, esse serviço visa avaliar continuamente e ininterruptamente os acessos aos sistemas críticos por meio de credenciais administrativas. Os eventos gerados serão analisados, sendo em caso positivo, transformados em um incidente de segurança da informação, obedecendo um processo rigoroso de gestão de eventos.

Monitoramento de Ataques Cibernéticos, o objetivo desse serviço é monitorar todo e qualquer tipo de ataque cibernético direcionado à CÂMARA MUNICIPAL DO RECIFE, através da análise de correlações de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, e em casos

positivos, transformados em um incidente de segurança da informação, obedecendo um processo rigoroso de gestão de eventos.

Resposta a Incidentes de Segurança Cibernética, o objetivo desse serviço é analisar, remediar, conter e documentar os eventos de segurança da informação, e caso descubra um ataque iminente, deve transformar em um incidente de segurança da informação. Esse serviço é executado, obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas.

Gestão de Proteção de Endpoints e Servidores de Rede, seu objetivo é proteger as estações de trabalho e os equipamentos servidores de rede corporativos, de forma eficiente, bloqueando a entrada e saída de informações críticas ou sensíveis, bem como examinar todo o conteúdo em busca de vírus, malwares, botnets ou outras ameaças avançadas.

Proteção de Mensageria Proativa, seu objetivo é proteger o serviço de mensageria utilizado pelos usuários internos, de forma eficiente, bloqueando a entrada e saída de e-mails indesejáveis, bem como examinar todo o conteúdo em busca de vírus, spams, phishing, botnets, ameaças avançadas, vazamento de informações, entre outros.

Inteligência Aplicada a Segurança Cibernética, tem por objetivo o monitoramento e a eliminação das informações, de qualquer tipo, relativa a CÂMARA MUNICIPAL DO RECIFE, suas autoridades e demais servidores que estejam trafegando ou sendo negociadas nas redes web consideradas perigosas ou seja nas Dark Web e Deep Web.

Serviços de Conscientização da Segurança da Informação, para conscientização de todos os usuários do parque tecnológico do CÂMARA MUNICIPAL DO RECIFE, sobre a importância de seguir as políticas de segurança da informação estabelecidas. Identificando proativamente os usuários que seriam vetores de ataques, e tornando-os elegíveis para um programa de capacitação interna, sobre boas práticas de segurança da informação no ambiente corporativo do CÂMARA MUNICIPAL DO RECIFE.

5. ESTIMATIVA DA QUANTIDADE DE BENS E/OU SERVIÇOS

A estimativa inclui:

ITEM	SERVIÇOS	QUAN
A	**SERVIÇO GERENCIADOS DE CIBERSEGURANÇA (NDR, EDR)** Gestão de Segurança para Infraestrutura e Sistemas Críticos Monitoramento de Ataques Cibernéticos Resposta a Incidentes de Segurança Cibernética Gestão de Segurança de Endpoints e Servidores de Rede Serviços de Segurança de Mensageria Proativa Inteligência Aplicada a Segurança Cibernética Serviços de Conscientização da Segurança da Informação **(Implementação de até 480 licenças de EDR e NDR**)	480

B	INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO	1
C	TREINAMENTO, SUPORTE E OPERAÇÃO DA SOLUÇÃO	1

Justificativa dos Quantitativos

Os quantitativos foram definidos com base em:

- Análise de demanda histórica e projeções futuras de crescimento.
- Necessidade de cobertura completa de todos os dispositivos e servidores da Câmara.
- Economia de escala ao contratar uma solução integrada.
- Prevenção de desperdício de recursos públicos através de uma contratação adequada e proporcional às necessidades reais.

6. LEVANTAMENTO DE MERCADO E ANÁLISE DAS SOLUÇÕES

6.1. CRITÉRIOS DE AVALIAÇÃO DAS ALTERNATIVAS

Para avaliarmos as alternativas de contratação da solução e embasarmos nossa decisão, levamos em conta os seguintes critérios:

Atendimento aos Requisitos – O mais importante dos critérios, uma vez que se os requisitos não forem atendidos, não teremos uma solução. Dentre eles a escalabilidade e a facilidade de uso têm uma relevância importante.

Custo – A relação custo x benefício deve apresentar-se favorável e compatível com a disponibilidade orçamentária.

Prazos – Os diferentes caminhos possíveis podem diferenciarem-se em muitos meses para sua consecução. Um projeto muito longo não atenderá ao requisito temporal de necessidades prementes.

Segurança – A segurança do ambiente, aplicativos e dados é condição indispensável à solução, uma vez que a continuidade do negócio e segurança de dados são inegociáveis. Por isso, o atendimento aos requisitos de segurança será condição decisiva na escolha da alternativa da mais adequada.

Riscos envolvidos – Critério que avalia e pondera os riscos de cada alternativa, dando subsídios para a melhor escolha.

Metodologia

- Pesquisa: Utilizou-se fontes confiáveis, incluindo Gartner, Forrester, IDC, relatórios de analistas e sites das empresas.
- Organização: Tabela comparativa destacando os principais aspectos de cada solução

6.2. DESCRIÇÃO DE CENÁRIOS

Cada cenário representa um perfil de solução para atender às necessidades da Câmara Municipal do Recife:

1. **Cenário 1**: Foco em proteção abrangente, com redundância e suporte técnico contínuo, visando segurança constante para todos os dispositivos e servidores.
2. **Cenário 2**: Integração com sistemas existentes e treinamento especializado, com foco no custo-benefício para garantir implementação e adaptação mais rápidas.
3. **Cenário 3**: Alta escalabilidade e compatibilidade com novas tecnologias, com garantia prolongada para atender à demanda de crescimento e modernização.
4. **Cenário 4**: Opção de segurança com menor custo, focando em funcionalidades essenciais e adequação mínima para atender às necessidades básicas.

6.3. ANÁLISE DOS CENÁRIOS

A tabela a seguir compara os cenários, considerando os seguintes critérios:

- Necessidade Administrativa: Preferência por proteção abrangente e resposta rápida.
- Utilização Pretendida: Segurança contínua e preventiva.
- Destinatário: Câmara Municipal do Recife.
- Objetivos: Redução de incidentes, conformidade legal e disponibilidade operacional.
- Eficiência e Economia: Preferência por soluções que combinem suporte técnico robusto e custo-benefício adequado.

6.4. EXAME COMPARATIVO DOS VALORES ESTIMADOS DAS SOLUÇÕES VIÁVEIS

As três soluções são detalhadas a seguir, com estimativa de custos ao longo de quatro anos:

Descrição da solução	Estimativa ao longo dos anos				Total
	Ano 1	Ano 2	Ano 3	Ano 4	
Solução Integrada de Cibersegurança (NDR, EDR) - **SOLUÇÃO TIPO 01**	R$ 785.280,00	R$ 738.720,00	R$ 738.720,00	R$ 738.720,00	R$ 3.001.440,00
Solução Integrada de Cibersegurança (NDR, EDR) - **SOLUÇÃO TIPO 02**	R$ 926.880,00	R$ 873.120,00	R$ 873.120,00	R$ 873.120,00	R$ 3.546.240,00
Solução Integrada de Cibersegurança (NDR, EDR) - **SOLUÇÃO TIPO 03**	R$ 891.600,00	R$ 844.800,00	R$ 844.800,00	R$ 844.800,00	R$ 3.426.000,00

Com base no que segue:

Cotação de mercado através de planilha enviada com os campos a serem preenchidos:

ITEM	SERVIÇOS	QUAN	UNI	VALOR UNITÁRIO	VALOR TOTAL	VALOR TOTAL
1	SERVIÇO GERENCIADOS DE CIBERSEGURANÇA (**480 licenças** de EDR e NDR confome TR)	480	LICENÇAS			
2	INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO **(Implementação de até 480 licenças de EDR e NDR)**	1	Unidades			
3	TREINAMENTO, SUPORTE E OPERAÇÃO DA SOLUÇÃO **(480 licenças de EDR e NDR)**	1	Unidades			
VALOR TOTAL GLOBAL						

Solução Tipo 1

ITEM	SERVIÇOS	QUAN	UNI	VALOR UNITÁRIO	VALOR TOTAL	VALOR TOTAL ANUAL
1	SERVIÇO GERENCIADOS DE CIBERSEGURANÇA (**480 licenças** de EDR e NDR confome TR)	480	LICENÇAS	R$ 112,00	R$ 53.760,00	R$ 645.120,00
2	INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO **(Implementação de até 480 licenças de EDR e NDR)**	1	Unidades	R$ 53.760,00	R$ 53.760,00	R$ 53.760,00
3	TREINAMENTO, SUPORTE E OPERAÇÃO DA SOLUÇÃO **(480 licenças de EDR e NDR)**	1	Unidades	R$ 19.000,00	R$ 19.000,00	R$ 228.000,00
				VALOR TOTAL GLOBAL	**R$ 926.880,00**	

Solução Tipo 2

Solução Tipo 3

Cada solução foi projetada com diferentes enfoques em funcionalidades e orçamento para se ajustar às necessidades específicas da CMR.

A análise considera:

ITEM	SERVIÇOS	QUAN	UNI	VALOR UNITÁRIO	VALOR TOTAL	VALOR TOTAL ANUAL
1	SERVIÇO GERENCIADOS DE CIBERSEGURANÇA	480	LICENÇAS	R$ 97,00	R$ 46.560,00	R$ 558.720,00

ITEM	SERVIÇOS	QUAN	UNI	VALOR UNITÁRIO	VALOR TOTAL	VALOR TOTAL ANUAL
1	SERVIÇO GERENCIADOS DE CIBERSEGURANÇA (**480 licenças** de EDR e NDR confome TR)	480	LICENÇAS	R$ 105,00	R$ 50.400,00	R$ 604.800,00
2	INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO **(Implementação de até 480 licenças de EDR e NDR)**	1	Unidades	R$ 46.800,00	R$ 46.800,00	R$ 46.800,00
3	TREINAMENTO, SUPORTE E OPERAÇÃO DA SOLUÇÃO **(480 licenças de EDR e NDR)**	1	Unidades	R$ 20.000,00	R$ 20.000,00	R$ 240.000,00
				VALOR TOTAL GLOBAL	**R$ 891.600,00**	

- Real necessidade da Administração: Prioridade em proteção abrangente e resposta rápida a incidentes.
- Utilização pretendida: Segurança contínua e preventiva para todos os dispositivos e servidores.
- Destinatário da contratação: Câmara Municipal do Recife.
- Objetivos: Redução de incidentes, conformidade legal, disponibilidade operacional.
- Meios mais eficientes, efetivos e econômicos: Solução com melhor custo-benefício e suporte técnico robusto.
- Prazo de garantia, entrega e validade: Preferência por soluções com garantias prolongadas e suporte contínuo.
- Durabilidade e ciclo de vida: Soluções que oferecem atualizações regulares e manutenção preventiva.
- Soluções mais adequadas às novas tecnologias: Preferência por plataformas escaláveis e compatíveis com tecnologias emergentes, garantindo modernidade e adequação ambiental.

Requisito	Sim	Não	N/A
Houve implantação da solução em outro órgão ou entidade da Administração Pública?	X		
Tendo em vista a análise de mercado, a solução atinge o resultado pretendido pela Administração da Câmara Municipal do Recife?	X		
A solução se mostra satisfatória aos resultados sob o aspecto da eficiência, efetividade e economia?	X		
A solução é aderente às normas licitatórias e à regulamentação interna da Câmara Municipal do Recife?	X		
Em caso de passagem de tecnologia e conhecimentos, futuramente, poderia a Câmara Municipal do Recife assumir a operação?	X		

6.5. DEFINIÇÃO E CONSIDERAÇÕES SOBRE A SOLUÇÃO ESCOLHIDA

Com base neste Estudo Técnico Preliminar, concluímos que Solução Tipo 1 foi definida como a opção ideal, combinando o NDR e EDR.

Esse tipo de solução atende aos critérios de proteção abrangente, escalabilidade e compatibilidade com

novas tecnologias, garantindo a conformidade com a LGPD e promovendo uma recuperação rápida em caso de incidentes.

A solução baseada nos softwares e serviços contidos no Tipo 1 será implementada para proteger um ambiente de:

- 30 Máquinas Virtuais (VMs) e aproximadamente.
- 450 endpoints da Câmara Municipal do Recife.

utilizando inteligência artificial e comprometimento contínuo para garantir uma proteção abrangente e eficaz.

SOLUÇÕES EXISTENTES:

Fabricante	Descrição	Link	Revendedor no Brasil
Darktrace	Utiliza inteligência artificial para detectar e responder a ameaças em redes empresariais.	Darktrace	Capterra, M3Corp
Vectra AI	A plataforma Cognito detecta e responde a ataques em redes de data center, IoT, e empresas.	Vectra AI	M3Corp, IT-One
Corelight	Combina tecnologias de código aberto como Suricata e Zeek para fornecer detecção e resposta em rede.	Corelight	Secure Soft, M3Corp
Palo Alto Networks	Oferece soluções NDR que utilizam aprendizado de máquina para detectar comportamentos anômalos.	Palo Alto Networks	ScanSource, M3Corp, IT-One
CrowdStrike	A plataforma Falcon fornece proteção baseada na nuvem e respostas rápidas a ameaças em endpoints.	CrowdStrike	Surfix, M3Corp, Secure Soft
SentinelOne	Utiliza inteligência artificial para fornecer prevenção, detecção e resposta automáticas a ameaças.	SentinelOne	Surfix, M3Corp, ISH Tecnologia
Carbon Black (VMware)	Oferece visibilidade e proteção contínuas para endpoints.	Carbon Black	M3Corp, Secure Soft
Cynet	Plataforma de segurança cibernética que integra EDR, NDR, e XDR (Extended Detection and Response).	Cynet	M3Corp, IT-One
Lumu	Oferece detecção e resposta contínuas usando uma abordagem de 'comprometimento contínuo'.	Lumu	Surfix

NDR (Network Detection and Response)
Darktrace
Site Oficial: Darktrace
Avaliações: Darktrace é bem avaliado por sua inteligência artificial avançada e capacidade de

detectar ameaças de forma autônoma. No Gartner Peer Insights, possui uma média de 4.6/5 estrelas.
Comparação: Comparado com outras soluções, Darktrace se destaca pela sua abordagem de aprendizado automático sem supervisão e pela capacidade de resposta autônoma. No entanto, pode ser mais caro em comparação com algumas soluções concorrentes como Corelight.

Vectra AI
Site Oficial: Vectra AI
Avaliações: Vectra AI recebe altas classificações pela sua plataforma Cognito, com foco em IA e análise comportamental. Tem uma média de 4.5/5 estrelas no Gartner Peer Insights.
Comparação: Vectra AI é frequentemente comparado favoravelmente com Darktrace, mas se diferencia com seu foco específico em ambientes de data center e IoT. Pode ser menos intuitivo para usuários novos em comparação com Darktrace.

Corelight
Site Oficial: Corelight
Avaliações: Corelight é elogiado por sua integração de tecnologias de código aberto como Zeek e Suricata. Possui uma média de 4.4/5 estrelas em avaliações de usuários.
Comparação: Corelight é uma escolha popular entre empresas que valorizam soluções de código aberto. Em comparação com Darktrace e Vectra AI, pode ser mais acessível, mas pode exigir mais conhecimento técnico para implementação.

Palo Alto Networks
Site Oficial: Palo Alto Networks
Avaliações: As soluções NDR da Palo Alto Networks são altamente avaliadas por sua eficácia e integração com outras ferramentas de segurança. Tem uma média de 4.6/5 estrelas no Gartner Peer Insights.
Comparação: Palo Alto Networks é frequentemente comparado com Cisco e Fortinet em termos de capacidade de resposta e integração com outros produtos de segurança. É considerado robusto, mas pode ser mais caro do que algumas outras opções.

Lumu
Site Oficial: Lumu
Avaliações: Lumu é elogiado pela sua abordagem de 'comprometimento contínuo' e facilidade de uso. Possui uma média de 4.8/5 estrelas em avaliações de usuários.
Comparação: Lumu é frequentemente comparado com Darktrace e Vectra AI por sua capacidade de detecção contínua. É considerado mais acessível e fácil de implementar, mas pode ter menos funcionalidades avançadas em comparação com alguns concorrentes.
EDR (Endpoint Detection and Response)

CrowdStrike

Site Oficial: CrowdStrike
Avaliações: CrowdStrike Falcon é altamente avaliado por sua proteção baseada na nuvem e resposta rápida a ameaças. Tem uma média de 4.8/5 estrelas no Gartner Peer Insights.
Comparação: CrowdStrike é frequentemente comparado com SentinelOne e Carbon Black. É considerado líder em detecção e resposta em endpoints, mas pode ser mais caro do que algumas outras soluções.

SentinelOne
Site Oficial: SentinelOne
Avaliações: SentinelOne é elogiado pela sua prevenção e resposta automáticas a ameaças com uso de IA. Possui uma média de 4.7/5 estrelas no Gartner Peer Insights.
Comparação: Comparado com CrowdStrike, SentinelOne é visto como igualmente eficaz, mas pode ser mais acessível. Alguns usuários preferem a interface de SentinelOne por sua simplicidade.

Carbon Black (VMware)
Site Oficial: Carbon Black
Avaliações: Carbon Black é bem avaliado por sua visibilidade contínua e proteção para endpoints. Tem uma média de 4.5/5 estrelas no Gartner Peer Insights.
Comparação: Em comparação com CrowdStrike e SentinelOne, Carbon Black é frequentemente elogiado por sua integração com a infraestrutura VMware, mas alguns usuários acham que pode ser menos intuitivo.

Cynet
Site Oficial: Cynet
Avaliações: Cynet é avaliado positivamente por sua integração de EDR, NDR e XDR. Possui uma média de 4.6/5 estrelas em avaliações de usuários.
Comparação: Cynet é comparado com soluções como CrowdStrike e SentinelOne, mas se destaca por sua abordagem integrada de segurança cibernética. É considerado uma boa opção para empresas que buscam uma solução tudo-em-um.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

Considerando todas as análises efetuadas e relatadas neste documento, a solução esperada é a contratação de empresa especializada para a prestação de serviços de segurança cibernética para a Câmara Municipal do Recife, que apresente produto e serviços com as seguintes características:

Eficácia

- **Proteção robusta de dados e endpoints**: A combinação de Lumu Defender e Sentinel One garante proteção completa dos dados críticos da CMR e de todos os endpoints, mitigando riscos de perda de dados, falhas de hardware, software e ataques cibernéticos. Isso assegura a continuidade das operações da Câmara.

- **Detecção e resposta proativa a ameaças**: Com inteligência artificial, as soluções detectam e respondem proativamente a ameaças em tempo real, minimizando o impacto de potenciais incidentes e garantindo uma rápida recuperação.
- **Recuperação rápida de desastres**: Em caso de desastres, como incêndios, inundações ou ataques cibernéticos, a solução permite a recuperação rápida dos dados e sistemas da CMR, minimizando o tempo de inatividade e o impacto nas atividades da instituição.
- **Conformidade com a LGPD**: Ambas as soluções auxiliam na conformidade com a Lei Geral de Proteção de Dados (LGPD), garantindo a proteção adequada dos dados pessoais armazenados e processados pela CMR.

Eficiência

- **Automação de processos de segurança**: As soluções automatizam diversos processos de detecção e resposta a incidentes, reduzindo a carga de trabalho da equipe de TI e permitindo que foquem em tarefas estratégicas.
- **Otimização do uso de armazenamento**: Utilizam técnicas de deduplicação e compressão de dados para reduzir significativamente o espaço de armazenamento necessário para backups, otimizando o uso de recursos e diminuindo custos.
- **Gerenciamento centralizado**: O painel de controle integrado permite uma gestão centralizada e eficiente de todas as operações de segurança, desde a detecção até a resposta e a remediação de incidentes, simplificando a operação e o controle da infraestrutura.
- **Redução de falsos positivos**: A inteligência artificial aprimorada reduz significativamente os falsos positivos, garantindo que a equipe de TI responda apenas a ameaças reais, otimizando o tempo e os recursos.

Efetividade

- **Aumento da produtividade**: Ao minimizar interrupções causadas por incidentes de segurança e garantir a disponibilidade dos dados, a solução contribui para um ambiente de trabalho mais produtivo e seguro, onde a equipe pode trabalhar sem interrupções causadas por perda de dados ou falhas de sistema.
- **Melhoria na tomada de decisões**: Relatórios detalhados e análises sobre o status de segurança permitem à CMR tomar decisões mais informadas sobre investimentos em infraestrutura e segurança da informação.
- **Reforço da imagem institucional**: A proteção robusta e a capacidade de resposta eficiente a incidentes reforçam a imagem institucional da CMR, demonstrando compromisso com a segurança da informação e a continuidade das operações.

Economicidade

- **Redução de custos com infraestrutura**: As soluções baseadas em software eliminam a necessidade de investimentos significativos em hardware adicional, reduzindo custos operacionais.
- **Diminuição de custos com mão de obra**: A automação de processos e o gerenciamento centralizado liberam a equipe de TI para se concentrar em atividades de maior valor agregado, reduzindo custos com mão de obra.

- **Minimização de perdas por indisponibilidade**: A proteção robusta e a rápida recuperação em caso de incidentes minimizam o impacto financeiro e operacional, evitando prejuízos significativos.

Ganhos Técnicos Adicionais

- **Escalabilidade**: A solução é facilmente escalável, permitindo a expansão do número de MVs e endpoints protegidos sem a necessidade de grandes investimentos adicionais.
- **Alta disponibilidade**: Ambas as soluções garantem alta disponibilidade com recursos avançados de detecção e resposta, mantendo a segurança contínua do ambiente da CMR.
- **Segurança avançada**: Com criptografia de dados em repouso e em trânsito, as soluções oferecem segurança robusta contra acesso não autorizado e outras ameaças cibernéticas.

Suporte técnico: Suporte técnico contínuo e qualificado está disponível para auxiliar a CMR na implementação, operação e resolução de problemas, garantindo a eficiência e a eficácia da solução implementada.

8. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

As pesquisas preliminares para fins de estabelecer a estimativa do valor da contratação, em atendimento ao Art. 18, inciso VI, da NLLC, de acordo com o item 6.4 EXAME COMPARATIVO DOS VALORES ESTIMADOS DAS SOLUÇÕES VIÁVEIS, apontam para custo total estimado da contratação, considerando a Solução Escolhida, é de R$ R$ 785.280,00 (setecentos e quarenta e sete mil setecentos e cinquenta), pagos anualmente.

Esta estimativa é compatível com os valores praticados no mercado, conforme levantamento realizado, e contempla os serviços necessários para a implementação e operação da solução.

Entretanto, após a escrita detalhada dos requisitos da solução e demais exigências da contratação, que será esmiuçada por ocasião da confecção do Termo de Referência, deve-se efetuar uma pesquisa de preços mais ampla, visando estabelecer um valor de referência mais assertivo para o processo licitatório.

9. JUSTIFICATIVA DO PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se recomenda o parcelamento da contratação devido aos seguintes aspectos:

- A solução deve ser integrada para garantir a proteção abrangente e evitar riscos ao conjunto do objeto.
- Economia de Escala: A contratação de um único fornecedor permitirá a obtenção de melhores condições comerciais e redução de custos de gestão de contratos.

- Com petição e Concentração de Mercado: A contratação de um fornecedor único evita a fragmentação que poderia limitar a competição e elevar os custos totais.

10. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

A. Proteção Robusta

Meta: Garantir a segurança total dos dados e endpoints da Câmara Municipal do Recife (CMR).

- Indicadores de Sucesso:
  - Redução de 95% nas falhas de segurança detectadas.
  - Nenhum incidente de perda de dados reportado.
  - Proteção contínua e atualizada contra ameaças cibernéticas emergentes.

B. **Detecção e Resposta Proativa a Ameaças**

Meta: Identificar e neutralizar ameaças de forma proativa e em tempo real.

- Indicadores de Sucesso:
  - Tempo médio de resposta a incidentes reduzido para menos de 1 hora.
  - Aumento de 80% na detecção de ameaças antes de causarem impacto significativo.
  - Diminuição em 90% do tempo de inatividade devido a incidentes de segurança.

C. Conformidade com a LGPD

Meta: Garantir que todas as operações estejam em conformidade com a Lei Geral de Proteção de Dados.

- Indicadores de Sucesso:
  - 100% de conformidade nas auditorias de segurança de dados.
  - Implementação completa de medidas de proteção de dados pessoais.
  - Nenhum incidente de vazamento de dados pessoais reportado.

D. Automação de Processos de Segurança

Meta: Otimizar a eficiência através da automação de processos de segurança.

- Indicadores de Sucesso:
  - Redução de 70% no tempo gasto em tarefas manuais de segurança.
  - Aumento de 50% na eficiência operacional da equipe de TI.
  - Implementação de automação em 90% dos processos de detecção e resposta a incidentes.

E. Melhoria na Tomada de Decisões

Meta: Fornecer insights detalhados e análises para decisões informadas sobre segurança e infraestrutura.

- Indicadores de Sucesso:
  - Disponibilização de relatórios de segurança detalhados mensais.
  - Implementação de análises preditivas para prevenção de ameaças futuras.
  - Melhoria de 30% na qualidade das decisões estratégicas de TI.

F. Reforço da Imagem Institucional

Meta: Demonstrar compromisso com a segurança da informação e a continuidade das operações.

- Indicadores de Sucesso:

- Melhorias percebidas na satisfação dos stakeholders em 25%.
- Aumento de 15% na confiança pública na CMR.
- Publicação de relatórios anuais de segurança e continuidade operacional.

G. Suporte Técnico Contínuo e Qualificado

Meta: Garantir suporte técnico contínuo e eficiente para todas as operações.

- Indicadores de Sucesso:
- Satisfação do cliente com suporte técnico acima de 90%.
- Redução de 50% no tempo de resolução de problemas.
- Disponibilidade de suporte 24/7, garantindo operação ininterrupta.

11. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PARA CONTRATAR

A contratação ora estudada resultará apenas na implantação de uma solução que otimizará os processos já existentes e trará mais agilidade e segurança às ações relativas a esses processos, mas não se converterá em nenhuma mudança radical às atividades das áreas envolvidas. Portanto, as providências a serem observadas são aquelas comuns a qualquer contratação. O treinamento, que naturalmente será dado aos usuários da solução contratada por ocasião da implantação do sistema, será suficiente para a assimilação das novas formas de execução das tarefas.

12. INDICAÇÃO DE CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não há.

13. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS

A solução de cibersegurança operando em nuvem reduz a necessidade de hardware físico local, mas ainda pode ter impactos ambientais devido ao consumo de energia dos Data Centers onde a solução será hospedada.

Medidas Mitigadoras:

- Otimização de Recursos: Configurar a solução para consumir apenas os recursos necessários, aproveitando as capacidades de escalabilidade e elasticidade da nuvem para minimizar o uso de energia e infraestrutura.

- Política de Logística Reversa: Garantir que qualquer equipamento de apoio local que se torne obsoleto seja devidamente descartado por meio de reciclagem e logística reversa.

Essas medidas ajudam a reduzir a pegada de carbono associada ao uso da solução em nuvem, promovendo uma abordagem mais sustentável para as operações de cibersegurança.

14. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO E POSICIONAMENTO CONCLUSIVO SOBRE A CONTRATAÇÃO ADEQUADA À DEMANDA

Declaração de Viabilidade: A contratação é viável e essencial para atender às necessidades de proteção de dados da Câmara Municipal do Recife. A solução escolhida oferece a melhor relação custo-benefício, assegurando eficácia, eficiência, efetividade e economicidade na proteção dos dados e na conformidade com a legislação vigente.

Posicionamento Conclusivo: A Solução Viável Tipo 1 é a mais adequada para a demanda apresentada, justificando-se pelos benefícios técnicos e econômicos que proporcionará, alinhando-se com os objetivos de modernização e segurança da Câmara Municipal do Recife.

15. APROVAÇÃO E ASSINATURAS

Consoante o art. da Resolução , de _ de , o Estudo Técnico Preliminar deverá ser aprovado e assinado pelo setor requisitante, pela área técnica e pela autoridade competente.

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
_____	Ricardo Williams Paixão Ferraz
Matrícula nº:	Matrícula nº: 1016059
Recife, em 07 de fevereiro de 2025.	Recife, em 07 de fevereiro de 2025.

(AUTORIDADE QUE APROVARÁ O ETP)
_____
Eriberto Rafael – 1º Secretário
Recife, em 07 de fevereiro de 2025.

Assinado digitalmente por
RICARDO WILLIAMS
PAIXAO FERRAZ
Data: 24/02/2025 09:21