ESTUDO TÉCNICO PRELIMINAR

INFORMAÇÕES BÁSICAS
Número do processo: 31.573/2024

Sumário

INTRODUÇÃO

Este Estudo Técnico Preliminar (ETP) tem por objetivo embasar a contratação de uma **Solução de Segurança da Informação** para a Administração Municipal de Cariacica, contemplando **Firewall de Próxima Geração, NDR (Network Detection and Response), XDR (Extended Detection and Response), Gestão de LOGs, Analítico de Rede, NIPS (Network Intrusion Prevention System) e ADC (Application Delivery Controller)**.

A elaboração do presente ETP atende aos ditames da **Lei nº 14.133/2021** (Nova Lei de Licitações e Contratos Administrativos), que preconiza a necessidade de planejamento, padronização e eficiência na contratação de bens e serviços, bem como a observância de outros normativos correlatos, tais como a **Lei Geral de Proteção de Dados (Lei nº 13.709/2018)** e os princípios gerais de Segurança da Informação.

A Subsecretaria de Tecnologia da Informação - SUBTI, faz parte da Secretaria Municipal de Finanças - SEMFI, é o órgão responsável por fazer a gestão e operação da Tecnologia e Segurança da Informação no âmbito da Administração Municipal de Cariacica, e cumprindo sua função, atua na modernização tecnológica e na proteção do parque computacional contra Ciberameaças.

A SUBTI administra a rede de dados de todos os prédios públicos, localizados no município de Cariacica, além de setores administrativos das Secretarias do Município.

DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

(art. 18 § 1º Inciso I)

O presente Estudo Técnico Preliminar (ETP) visa analisar as soluções tecnológicas atualmente utilizadas nos órgãos da Administração Pública de Cariacica e demais entes para Modernização da Segurança Cibernética e Privacidade de Dados de modo adequado.

Cumnpre informar que a Prefeitura de Cariacica, em 2024, adquiriu dois firewalls do fabricante Hillstone modelo SG-6000-A5500 para substituir equipamentos anteriores (APPLIANCE APL UTM BB 2000 BBHWUTM443 e APPLIANCE APL UTM BB 10000 BBHWUTM) que apresentavam baixa capacidade

de processamento e qualidade técnica deficiente em proteção cibernética. Essa substituição representou um avanço significativo na segurança da informação do município.

Contudo, o cenário de ameaças cibernéticas é dinâmico e crescente, assim como as demandas por conectividade e serviços digitais oferecidos pela Prefeitura à população a exemplo do agendamento de consultas médicas, da disponibilização do boletim escolar das unidades da rede de ensino do município, da disponibilização do diário eletrônico, das disponibilização do portal de transparência da gestão municipal, da aquisição de bens e serviços à devida continuidade das atividades da Prefeitura via o portal de compras públicas, da disponibilização dos serviços de alvarás e pagamento de taxas e tributos.

A SUBTI, por meio da Gerência de Segurança da Informação (GSI), está empenhado na implementação de uma nova política de segurança cibernética e privacidade dos dados no âmbito dos projetos do órgão.

A Prefeitura Municipal de Cariacica, atualmente possui um grande conjunto de dados estruturados e não estruturados referentes a Administração do Município, em todos os seus servidores de Sistemas, bancos de dados e de arquivos. Além disso, existe uma grande quantidade de dados em arquivos nas estações de trabalho.

Embora a infraestrutura de Segurança Cibernética da PMC, possua alguns mecanismos de proteção, existem riscos que necessitam ser mitigados, objetivando a resolução de problemas como:

Ameaças Cibernéticas Crescentes: A complexidade de ataques digitais (ransomware, phishing, trojans, etc.) vem aumentando, tornando insuficientes soluções pontuais de segurança para mitigar riscos.

Proteção de Dados Sensíveis: A Administração Municipal de Cariacica lida com dados críticos de diversas áreas (saúde, educação, arrecadação, entre outras), cuja perda ou divulgação indevida afeta diretamente a população e a continuidade de serviços.

Exposição em Ambientes Virtuais: A adoção de virtualização e a disseminação de máquinas virtuais (VMs) sem um mecanismo efetivo de proteção contra movimentos laterais representam pontos de vulnerabilidade na infraestrutura de TI.

Falta de Microsegmentação: Redes amplas, segmentadas de forma tradicional ou insuficiente, podem permitir que um invasor se mova livremente após um ponto de acesso inicial, aumentando o impacto potencial de ataques cibernéticos.

Governança e Auditoria Insuficientes: A falta de integração das ferramentas de segurança prejudica a visibilidade, a correlação de eventos, a conformidade legal e a capacidade de geração de relatórios de auditoria.

Sobre os dados e informações da Administração Pública, um possível vazamento acarreta inúmeras consequências negativas, colocando em risco a privacidade e segurança dos munícipes e contribuintes. Dentre as inúmeras consequências negativas, vale destacar algumas das principais:

Risco Legal e Regulatório

- **Multas e Sanções**: A legislação brasileira, especialmente a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), prevê penalidades que podem incluir advertências e multas que podem chegar a 2% do faturamento da entidade (ou, no caso de entes públicos, penalidades administrativas específicas).
- **Ações Judiciais**: Cidadãos prejudicados podem ingressar na justiça requerendo indenizações por danos morais e materiais, o que pode gerar custos elevados e desgaste institucional.

Perda de Credibilidade e Danos à Imagem

- **Erosão da Confiança da População**: Um vazamento de dados pode comprometer a relação de confiança entre os munícipes e a prefeitura, dificultando futuras iniciativas e programas municipais.
- **Repercussão Negativa na Mídia**: A exposição negativa na imprensa local e nacional pode prejudicar a reputação do município, impactando a percepção pública sobre a qualidade dos serviços prestados.

Exposição de Informações Sensíveis

- **Dados de Natureza Pessoal**: Informações como nomes, endereços, números de documentos (RG, CPF) e dados de saúde podem cair em mãos de criminosos, abrindo margem para golpes e fraudes.
- **Segurança de Grupos Vulneráveis**: Dados referentes a crianças, idosos ou pessoas em situação de vulnerabilidade podem ser usados de forma indevida, acarretando riscos adicionais à integridade dessas populações.

Impacto na Prestação de Serviços Públicos

- **Interrupção das Atividades**: O vazamento pode obrigar a suspensão de sistemas ou serviços de TI, resultando em prejuízos à continuidade do atendimento ao cidadão.

- **Necessidade de Reestruturação**: Em caso de ataque cibernético, a equipe de TI pode ter de reconstruir ou migrar sistemas críticos, demandando tempo, recursos e comprometendo projetos em andamento.

Prejuízos Financeiros

- **Custos de Contenção e Reparação**: Inclui gastos com consultorias de segurança, reparos de sistemas, notificação de cidadãos, além da implementação de novas medidas para evitar incidentes futuros.
- **Redirecionamento de Orçamento**: Recursos que poderiam ser investidos em educação, saúde ou infraestrutura precisam ser alocados em ações emergenciais de recuperação e mitigação do incidente.

Possível Uso Criminoso das Informações

- **Fraudes e Golpes**: Informações pessoais podem ser utilizadas para a abertura de contas bancárias fraudulentas, solicitação de crédito ou outros delitos, colocando a população em risco.
- **Risco de Phishing e Engenharia Social**: Dados vazados podem ser combinados a outros elementos para criar ataques de engenharia social, facilitando novos golpes contra cidadãos e servidores do município.

Responsabilização de Gestores e Servidores

- **Implicações Administrativas**: Servidores públicos e gestores podem responder a processos disciplinares, caso fique caracterizada omissão ou negligência na proteção de dados.
- **Comprometimento de Carreira**: A perda de confiança e possíveis punições podem afetar a trajetória profissional de gestores e equipes envolvidas na gestão de dados.

Suscetibilidade a Novos Ataques

- **Retaliações e Exploração de Brechas**: Se a vulnerabilidade não for corrigida imediatamente, invasores podem explorar novamente as falhas, agravando ainda mais a exposição de dados.
- **Escalonamento do Incidente**: Um primeiro vazamento pode encorajar outros ataques, sobretudo se criminosos percebem que não houve melhorias concretas na segurança do ambiente.

Diante dessas consequências e diante de um ambiente tão específico da Administração de Cariacica, onde a segurança dos dados e a privacidade, são fatores primordiais, é fundamental adotar medidas eficazes de Segurança Cibernética, garantindo um ambiente digital mais seguro e protegido para manuseio dessa informação e sua abundante importância.

Tal cenário torna-se desafiador tendo em vista que a Administração de Cariacica, pois muito embora a SUBTI tenha implementado mecanismos de Segurança da Informação nos últimos anos, ainda precisa efetuar a tratativa de riscos residuais, buscando Excelência na Gestão da Segurança Cibernética.

PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAIS

(art. 18 § 1º Inciso II)

A pretendida aquisição se faz pela necessidade de investimentos em segurança da informação sendo inicialmente dividida da seguinte forma:

SEME - Secretaria Municipal de Educação - PCW00417.2025-30

SEMUS - Secretaria Municipal de Saúde - PCW00428.2025-24

A pretendida aquisição além dos recursos financeiros das duas Secretarias citadas acima, terá recursos oriundos da SEMFI (Secretaria Municipal de Finanças) e SEMDEFES (Secretaria Municipal de Defesa Social), porém, em se tratando de Ata de Registro de Preços; considerando o período de realização de todo o trâmite processual até a finalização e publicação da Ata de Registro de Preços, neste sentido, a inclusão da pretendida aquisição junto ao Plano de Contratação Anual em relação a SEMFI e SEMDEFES ocorrerá no ano de 2026.

REQUISITOS DA CONTRATAÇÃO

(art. 18 § 1º Inciso III)

A contratação deverá atender aos seguintes requisitos:

3.1.Requisitos da Solução de Firewall (Equipamentos e Licenças):

- Aquisição de novos appliances de firewall da marca Hillstone, de modelos que representem uma atualização e/ou ampliação de capacidade em relação aos SG-6000-A5500 existentes, ou aquisição de modelos equivalentes para redundância e expansão em outros pontos da rede.
- Compatibilidade e interoperabilidade total com os firewalls Hillstone SG-6000-A5500 já em operação, permitindo gerenciamento centralizado e políticas de segurança coesas.
- Funcionalidades de Next-Generation Firewall (NGFW), incluindo, no mínimo: Stateful Packet Inspection, VPN (IPSec e SSL), Intrusion Prevention System (IPS), Controle de Aplicações, Filtro de Conteúdo Web, Antivírus de Gateway, Anti-Spam, Sandboxing (preferencialmente em

nuvem ou appliance dedicado, conforme TR anexo), Proteção contra Ameaças Avançadas Persistentes (APT), e Defesa contra DDoS.

- Alta capacidade de *throughput* de *firewall*, IPS, NGFW e VPN, dimensionada para as necessidades atuais e com projeção de crescimento para os próximos 5 anos.
- Interfaces de rede de alta velocidade (ex: 1GbE, 10GbE SFP+), conforme a necessidade de conexão com a infraestrutura de rede existente e futura.
- Suporte a Alta Disponibilidade (High Availability - HA) em modo Ativo/Passivo ou Ativo/Ativo;
- Controle de aplicações e usuários com inspeção profunda de pacotes (DPI) e bloqueio de ameaças avançadas com Segmentação de rede e VPN segura;
- NDR (Network Detection and Response) com Detecção de atividades anômalas em tempo real e Monitoramento de tráfego em toda a rede, buscando indicadores de comprometimento;
- XDR (Extended Detection and Response) com Consolidação de dados de endpoints, rede, nuvem e aplicações e Correlação inteligente de eventos e automação de resposta a incidentes.
- Gestão de LOGs (SIEM / Syslog / Ferramenta Equivalente) com Coleta e análise centralizada de eventos e Criação de dashboards, geração de alertas e relatórios de auditoria.
- Analítico de Rede (Network Analytics) com Visão detalhada do fluxo de dados, aplicações e padrões de tráfego e Identificação de gargalos, intrusões e comportamentos fora do normal.
- NIPS (Network Intrusion Prevention System) com Prevenção de intrusões e ataques em nível de rede e Atualização contínua de assinaturas de ameaças.
- ADC (Application Delivery Controller) com Balanceamento de carga e alta disponibilidade de serviços e Otimização e aceleração de aplicações críticas para o município.
- Criação de segmentos lógicos de rede para limitar a movimentação lateral de invasores com a aplicação de políticas de segurança específicas para cada segmento, isolando ambientes e serviços estratégicos.
- Proteção de Máquinas Virtuais contra Movimentação Lateral com solução focada em ambientes virtualizados (VMs), monitorando o tráfego inter-VM mantendo as políticas de isolamento e detecção de comportamentos suspeitos em cada instância virtual.
- Licenciamento para todas as funcionalidades de segurança descritas, com validade mínima de 36 (trinta e seis) ou 60 (sessenta) meses, a ser definido na fase de Termo de Referência.
- Garantia de hardware dos equipamentos pelo mesmo período do licenciamento.
- Fornecimento de todas as atualizações de firmware e assinaturas de segurança durante o período de vigência do contrato.

3.2.Escopo dos Serviços que serão realizados:

- **Instalação e Configuração:** Instalação física e lógica dos novos equipamentos, configuração em HA (se aplicável), integração com a rede existente e com os firewalls Hillstone atuais.
- **Migração:** Migração das políticas e configurações dos firewalls existentes (ou parte delas) para a nova solução, conforme o plano de ampliação, garantindo a continuidade operacional e

minimizando o impacto aos usuários.

- **Treinamento:** Capacitação da equipe técnica da SUBTI na operação, gerenciamento e troubleshooting da nova solução de firewall Hillstone (abrangendo os novos modelos e funcionalidades).
- **Suporte Técnico:** Suporte técnico especializado do fabricante ou de representante autorizado, em português, com níveis de serviço definidos (ex: 8x5xNBD, 24x7x4), incluindo acesso a atualizações, base de conhecimento e especialistas. O TR anexo menciona "Serviço de Suporte Técnico 24x7" e "Serviço de Suporte Técnico Especializado", que podem servir de base para a definição.

3.3.Requisitos de Padronização e Continuidade:

- A solução ofertada deve ser do fabricante Hillstone Networks, visando à padronização da infraestrutura de segurança.
- Justificativa: A padronização com a tecnologia Hillstone é fundamental para:
  - **Aproveitamento do Conhecimento Adquirido:** A equipe técnica da SUBTI já possui experiência e treinamento na plataforma Hillstone desde 2024, reduzindo a curva de aprendizado e otimizando o tempo de resposta a incidentes e a gestão da solução.
  - **Facilidade na Continuidade da Operação:** A familiaridade com a interface, lógicas de configuração e troubleshooting simplifica a gestão do ambiente, garante maior estabilidade e facilita a integração entre os equipamentos antigos e novos.
  - **Otimização de Recursos:** Reduz a necessidade de treinamentos extensivos em novas plataformas, custos com múltiplas ferramentas de gerenciamento e complexidade na administração do ambiente de segurança.
  - **Interoperabilidade:** Garante compatibilidade total entre os firewalls existentes e os novos, permitindo políticas de segurança unificadas e gerenciamento centralizado eficiente.

3.4. Implantar um Ecossistema Unificado de Segurança: Assegurar múltiplas camadas de proteção – desde o perímetro até o tráfego interno, infraestrutura virtualizada e aplicações.

3.5. Evitar e Detectar Ameaças em Tempo Real: Capacitar a equipe de TI a identificar e responder rapidamente a atividades maliciosas (via NDR, XDR, NIPS) e a isolar incidentes por meio de Microsegmentação.

3.6. Proteger Máquinas Virtuais contra Movimentações Laterais: Implementar políticas de segurança específicas para ambientes virtualizados, limitando a propagação de ameaças dentro do data center.

3.7. Melhorar a Governança de TIC: Centralizar a gestão de segurança e otimizar processos de auditoria, com geração de logs e relatórios integrados (Gestão de LOGs/SIEM e Analítico de Rede).

3.8. A solução deverá contemplar, de maneira integrada, os seguintes componentes/ferramentas:

a. **Firewall de Próxima Geração (NGFW)**

i. Controle de aplicações e usuários;
ii. Inspeção profunda de pacotes (DPI) e bloqueio de ameaças avançadas;
iii. Segmentação de rede e VPN segura.

b. **NDR (Network Detection and Response)**
   i. Detecção de atividades anômalas em tempo real;
   ii. Monitoramento de tráfego em toda a rede, buscando indicadores de comprometimento.

c. **XDR (Extended Detection and Response)**
   i. Consolidação de dados de endpoints, rede, nuvem e aplicações;
   ii. Correlação inteligente de eventos e automação de resposta a incidentes.

d. **Gestão de LOGs (SIEM / Syslog / Ferramenta Equivalente)**
   i. Coleta e análise centralizada de eventos;
   ii. Criação de dashboards, geração de alertas e relatórios de auditoria.

e. **Analítico de Rede (Network Analytics)**
   i. Visão detalhada do fluxo de dados, aplicações e padrões de tráfego;
   ii. Identificação de gargalos, intrusões e comportamentos fora do normal.

f. **NIPS (Network Intrusion Prevention System)**
   i. Prevenção de intrusões e ataques em nível de rede;
   ii. Atualização contínua de assinaturas de ameaças.

g. **ADC (Application Delivery Controller)**
   i. Balanceamento de carga e alta disponibilidade de serviços;
   ii. Otimização e aceleração de aplicações críticas para o município.

h. **Microsegmentação**
   i. Criação de segmentos lógicos de rede para limitar a movimentação lateral de invasores;
   ii. Aplicação de políticas de segurança específicas para cada segmento, isolando ambientes e serviços estratégicos.

i. **Proteção de Máquinas Virtuais contra Movimentação Lateral**
   i. Solução focada em ambientes virtualizados (VMs), monitorando o tráfego inter-VM;
   ii. Políticas de isolamento e detecção de comportamentos suspeitos em cada instância virtual.

3.9. Observância à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)

- Implementação de medidas técnicas e administrativas que assegurem o tratamento adequado de dados pessoais;

- Geração de registros e relatórios que facilitem a prestação de contas junto à Autoridade Nacional de Proteção de Dados (ANPD).

3.10. Compatibilidade e Integração

- Interface com sistemas legados, diretórios de autenticação (e.g., Active Directory) e plataformas de virtualização existentes;
- Suporte a protocolos e padrões abertos, permitindo evolução tecnológica sem dependência de fornecedor único.

3.11. Escalabilidade e Flexibilidade

- Possibilidade de acréscimo de módulos e licenças, acompanhando o crescimento da infraestrutura;
- Suporte a ambientes híbridos (on-premises, nuvem pública e/ou nuvem privada).

3.12. Gestão Simplificada e Centralizada

- Portal ou console unificado para administração de políticas de segurança;
- Dashboards customizáveis para monitoramento em tempo real de incidentes e desempenho.

3.13. Suporte Técnico Especializado

- Garantia de updates e manutenção com Service Level Agreement (SLA) adequado;
- Disponibilidade de treinamento e consultoria para equipes de TI.

ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

(art. 18 § 1º Inciso IV)

Tabela com as quantidades inicialmente projetada

Item	Descrição	PartNumber	Tipo	Qtd
01	Solução de Firewall de Controle de Aplicação	SG-6000-A5500-AD-IN60	HW	04
02	Solução de Firewall de Perímetro	SG-6000-A3800-AD-IN60	HW	04
03	Solução de Detecção e Resposta de Rede	BDS-IV08-SW-IN60	SW	02
04	Solução de Detecção e Resposta Estendida	SG-6000-ISC6210-BP-IN	SW	02
05	Solução de Balanceamento de Circuito	SG-6000-AX1200S-IN60	HW	02
06	Solução de Gerenciamento Centralizado de Firewall	SG-6000-vHSM-IN36	SW	02
07	Solução de Centralização de Logs	SG-6000-VHSA-2-IN36	SW	02
08	Solução Analítica de Rede	CloudV-Pro-5000	SW	08
09	Treinamento para Solução de Firewall	N.A	SE	02

10	Treinamento para Solução de Detecção e Resposta de Rede	N.A	SE	02
11	Treinamento para Solução de Detecção e Resposta Estendida	N.A	SE	02
12	Treinamento para Solução de Balanceamento de Circuito	N.A	SE	02
13	Treinamento para Solução Centralização de Logs	N.A	SE	02
14	Treinamento para Solução Analítica de Rede	N.A	SE	02
15	Serviço de Operação Assistida da Solução de Segurança	N.A.	SE	14
16	Serviço de Suporte Técnico 24x7	N.A.	CHAMADO	200
17	Serviço de Suporte Técnico Especializado	N.A.	UST	20
18	Instalação e Configuração de Firewall	N.A.	SE	08
19	Instalação e Configuração de Solução de Detecção e Resposta de rede	N.A.	SE	02
20	Instalação e Configuração de Solução de Detecção e Resposta Estendida	N.A.	SE	02
21	Instalação e Configuração de Solução de Balanceamento de Circuito	N.A.	SE	02
22	Instalação e Configuração de Solução de Gerenciamento Centralizado de Firewall	N.A.	SE	08
23	Instalação e Configuração de Solução de Centralização de Logs	N.A.	SE	02
24	Configuração e Parametrização de Analítico de Rede	N.A.	SE	02

LEVANTAMENTO DE MERCADO

(art. 18 § 1º Inciso V)

A tabela a seguir traz alguns dos principais **fabricantes** com soluções que abrangem **Firewall, NDR, XDR, Gestão de LOGs, Análise de Rede (Analytics), NIPS, ADC, Microsegmentação** e **Proteção de Máquinas Virtuais (movimentação lateral)**. Cada linha apresenta o **produto** (ou conjunto de produtos) e fornece um breve descritivo dos **principais recursos** e das **capacidades críticas** de cada oferta.

Fabricante	Produtos Principais	Principais Recursos	Capacidades Críticas
Palo Alto Networks	- Next-Generation Firewall (PA Series / VM-Series) - Cortex XDR	- Firewall com inspeção profunda (DPI) e controle de aplicações.	- Visibilidade Integrada: combina firewall, NDR, XDR e microsegmentação

	- Cortex Data Lake - Prisma Cloud (Microsegmentação e proteção de VMs)	- XDR que unifica dados de endpoint, rede, e nuvem para detecção e resposta. - Microsegmentação e proteção de workloads em ambientes de cloud/híbrido via Prisma. - Coleta centralizada de logs e análises avançadas.	para reduzir lacunas de segurança. - Automações por IA/ML para detecção de ameaças. - Proteção de VMs (VM-Series) contra movimentos laterais. - Escalabilidade em infraestruturas locais e em nuvem.
Fortinet	- FortiGate (NGFW / NIPS) - FortiNDR - FortiEDR / FortiXDR - FortiSIEM / FortiAnalyzer (Logs e Analytics) - FortiADC - FortiMicroseg (Microsegmentação)	- NGFW com IPS e controle de aplicativos integrados. - NDR para análise de tráfego e detecção de ameaças avançadas. - XDR para unificar eventos de endpoint e rede. - SIEM e Analyzer para gestão de logs e relatórios de conformidade. - ADC para balanceamento de carga.	- Security Fabric: integra diversos módulos (Firewall, NDR, XDR, SIEM) em painel único. - Microsegmentação combinada com switches/SDN Fortinet. - Alto Desempenho para tráfego crítico. - Vasto Ecossistema de produtos, ampliando opções de expansão.
Cisco	- Firepower NGFW / IPS - SecureX (XDR e orquestração) - Stealthwatch (Secure Network Analytics / NDR) - Tetration/ACI (Microsegmentação) - Secure ADC (antigo ACE)	- NGFW com IPS, controle de aplicativos e integração com ambientes Cisco. - NDR (Stealthwatch) para análise de comportamento e detecção de anomalias em rede. - XDR via SecureX, correlacionando dados de diferentes vetores. - ACI/Tetration para microsegmentação de data center.	- Integração Profunda com infraestrutura Cisco (switches, roteadores, Wi-Fi). - Visão Unificada (SecureX) para eventos de segurança. - Microsegmentação avançada e Zero Trust em data center. - ADC para alta disponibilidade e entrega

			de aplicações de missão crítica.
Check Point	- Quantum Security Gateways (NGFW / NIPS) - CloudGuard (NDR, microsegmentação) - Harmony Endpoint (XDR) - Infinity SOC (Analytics e orquestração)	- NGFW e IPS com foco em inspeção em múltiplas camadas. - NDR e microsegmentação para ambientes híbridos e nuvem via CloudGuard. - XDR (Harmony) unifica segurança de endpoints, rede e usuários. - Infinity SOC para análise de ameaças e correlação de eventos.	- Infinity Architecture integra diferentes soluções em console único. - Alto Grau de Proteção em ambientes multi-cloud. - Microsegmentação robusta para workloads em nuvem. - Detecta Ameaças Avançadas (APT) via inteligência de mercado e IA.
Vmware	- NSX (Microsegmentação e Firewall Distribuído) - Carbon Black (XDR) - vRealize Log Insight (Gestão de Logs e Análises)	- Microsegmentação NSX para isolar tráfego entre VMs e prevenir ataques laterais. - Firewall Distribuído para políticas granulares em cada VM. - Carbon Black (XDR) com proteção de endpoint/VM. - Log Insight para coleta e análise de eventos em infra VMware.	- Foco Profundo em Virtualização (vSphere, vCenter). - Proteção de VMs nativa contra movimentação lateral. - Integração com nuvens híbridas e containers. - Políticas Zero Trust aplicáveis de forma automática e escalável.
Trend Micro	- TippingPoint (NIPS) - Deep Discovery (NDR) - Vision One (XDR) - Deep Security / Cloud One (Proteção de VMs e microsegmentação)	- NIPS com TippingPoint, proteção de rede em tempo real. - NDR (Deep Discovery) para detecção de ameaças avançadas. - XDR (Vision One) consolidando alertas de endpoints, rede e e-mail. - Deep Security para	- Detecção Avançada de APTs (sandboxing e reputação de ameaças). - Visão Unificada em Vision One (XDR). - Proteção de VMs e containers em múltiplas plataformas. - Abordagem Preventiva

		servidores e VMs com microsegmentação lógica.	(IPS + NDR) diminui janelas de exposição.
F5	- BIG-IP (ADC, L4-L7 Firewall, WAF) - Advanced WAF - SSL Orchestrator - Integrações para NDR e microsegmentação com parceiros	- ADC para balanceamento, offload de SSL e disponibilidade de aplicações. - Firewall L4-L7 e WAF para proteção de tráfego HTTP/HTTPS. - SSL Orchestrator para visibilidade de tráfego criptografado. - Pode integrar-se a soluções de NDR/XDR e microsegmentação de terceiros.	- Especialista em Camada de Aplicação (balanço, segurança e aceleração). - Alto Desempenho em inspeção SSL e proteção de APIs. - Integrações com ecossistemas variados (Cisco, VMware, etc.). - Oferece Módulos que podem compor firewall e WAF com políticas avançadas.

Destaques e Considerações:

1. **Firewall e NIPS**
   - A maioria dos fabricantes listados possui soluções que combinam **NGFW** (Next-Generation Firewall) e **NIPS** para inspeção profunda de pacotes (DPI) e prevenção de intrusões, atendendo às necessidades de proteção de perímetro e tráfego interno.
2. **NDR e XDR**
   - Ferramentas como **Cortex XDR** (Palo Alto), **FortiNDR / FortiXDR** (Fortinet), **SecureX/Stealthwatch** (Cisco), **Harmony/CloudGuard** (Check Point), **Deep Discovery / Vision One** (Trend Micro) e **Carbon Black** (VMware) oferecem capacidades de detecção e resposta a ameaças em diferentes vetores (rede, endpoint, nuvem).
3. **Gestão de LOGs e Análise de Rede**
   - Geralmente fornecidas por módulos SIEM (FortiSIEM, vRealize Log Insight, Infinity SOC, etc.), ou plataformas analíticas que unificam eventos de segurança e desempenho de rede, garantindo maior visibilidade e auditoria.
4. **ADC**
   - Fabricantes como **F5** (BIG-IP) e **Fortinet** (FortiADC) se destacam em soluções de balanceamento de carga, alta disponibilidade e aceleração de aplicações, protegendo camada de aplicação (L7) e otimizando performance.
5. **Microsegmentação e Proteção de Máquinas Virtuais**

- **VMware NSX** e **Palo Alto Prisma** são referências em microsegmentação de ambientes virtualizados, restringindo o movimento lateral de atacantes.
- **Trend Micro Deep Security**, **FortiMicroseg** e **Check Point CloudGuard** também oferecem micro segmentação e controle refinado para VMs e containers.

6. **Capacidades Críticas**
   - **Visão Integrada**: A consolidação de Firewall, NDR, XDR e microsegmentação em um ecossistema unificado reduz lacunas e facilita a orquestração de incidentes.
   - **Proteção de Ambientes Híbridos**: Fundamental para organizações que usam data centers tradicionais e nuvens públicas/privadas.
   - **Escalabilidade e Automação**: A capacidade de crescer em ambientes complexos e automatizar detecções/respostas a ameaças é essencial para diminuir o tempo de exposição e reduzir custos operacionais.
   - **Gerenciamento de Logs e Conformidade**: Ferramentas de SIEM e análise de rede asseguram auditoria adequada e aderência a regulações (LGPD, ISO 27001, etc.).

Com a Análise de Mercado e tecnologias podemos verificar que as Compras Públicas desses produtos são comuns, nesse sentido seguem algumas contratações similares. Estas serão utilizadas também para compor a estimativa de preços.

TRIBUNAL REGIONAL FEDERAL 3 REGIAO
Contratação de empresa especializada para fornecimento de solução firewall NGFW (Next Generation Firewall) composta por aquisição de equipamentos principais e de contingência, licenciamento de funcionalidades, serviço de implantação, serviço de garantia estendida de serviço e bens, pelo período de 60 (sessenta) meses, e serviço de operação e sustentação de ambiente.
https://pncp.gov.br/app/editais/59949362000176/2024/100

AGÊNCIA REGULADORA DE SERVIÇOS PÚBLICOS DO ESTADO DE SÃO PAULO - ARSESP
O objeto do presente instrumento é a contratação de solução de proteção de redes com características de Next Generation Firewall - NGFW, com serviços de instalação, configuração, treinamento e garantia on-site de 60 (sessenta) meses.
https://pncp.gov.br/app/contratos/02538438000153/2024/30

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA-CADE
Aquisição de equipamentos de proteção de rede, denominados Firewalls de Próxima Geração (Next Generation Firewall - NGFW) com proteção DNS, abrangendo serviços de planejamento, implementação e execução da migração entre equipamentos, solução de gerência centralizada e solução de armazenamento de logs com garantia e suporte técnico por 60 (sessenta) meses e

fornecimento de toda documentação técnica gerada durante o período de implantação da solução e contra
https://pncp.gov.br/app/editais/00418993000116/2024/17

CONSELHO FEDERAL DE MEDICINA
Aquisição de solução de firewall com gerenciamento unificado de ameaças (NGFW) e garantia técnica, serviços de instalação e configuração, treinamento oficial e suporte técnico on-site pelo prazo de 60 (sessenta) meses, conforme as especificações e as condições estabelecidas no Termo de Referência.
https://pncp.gov.br/app/editais/33583550000130/2023/69

TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS
Objeto: Contratação de empresa especializada no fornecimento, instalação e configuração de Firewall com soluções de gerenciamento de dispositivo de rede para segurança de dados em ambiente de Data Center, composta por Firewall e Software, de acordo com as condições, especificações e quantidades constantes do Anexo Único do Termo de Referência, através do Pregão Eletrônico 017/2023.
https://portal.tce.go.gov.br/documents/20181/711446/PE017SEGURAN%C3%87AFIREWALL.pdf/c990438d-83e3-47d7-8c63-0ddff4b694c7

PROCURADORIA GERAL DO ESTADO DO AMAPÁ
Objeto: Aquisição de Solução Integrada de Firewall Composta de Hardware e Software de Segurança da Informação (PRODAP), através do Pregão 190/2023.
https://pncp.gov.br/app/editais/01002322000132/2023/50

MINISTÉRIO DA CULTURA
Objeto: Registro de preços para aquisição de uma solução de proteção de rede Next Generation Firewall (NGFW) com garantia e suporte, através do Pregão Eletrônico 09/2023.
http://www.comprasnet.gov.br/acesso.asp?url=/edital-420001-5-00009-2023

BANCO DO BRASIL - CESUP
Objeto: Registro de Preços para aquisição de até 185.000 (cento e oitenta e cinco mil) licenças de software de segurança XDR (Extended Detection and response) especializado em detecção e resposta a incidentes de segurança, Anti-malware e anti-spyware, com garantia técnica pelo período de 60 (sessenta) meses, pelo número do processo 2023/03977 e número de licitação 1026007, através do endereço.
https://licitacoes-e.com.br.

SUPREMO TRIBUNAL FEDERAL

Objeto: Objeto: Pregão Eletrônico - Contratação de empresa para fornecimento de subscrições de solução de detecção e resposta estendida a incidentes de segurança cibernética - XDR (Extended Detection and response), serviços de monitoramento, prevenção, detecção e resposta a ameaças de nova geração, contemplando operação, gestão, suporte e atualizações da solução XDR (Extended Detection and response) e serviços de treinamento

Link: https://www.comprasnet.gov.br/acesso.asp?url=/edital-40001-5-90005-2024

MINISTERIO PUBLICO DA UNIAO

O objeto da presente licitação é o Registro de Preços para a contratação de empresa especializada no fornecimento de solução para expansão e atualização tecnológica dos softwares de segurança de aplicações e balanceamento de carga das plataformas F5 BIG-IP, incluindo aquisição de novas instâncias e serviços de apoio e suporte, para atendimento a demanda da Escola Superior do Ministério Público da União – ESMPU, conforme condições, quantidades e exigências estabelecidas

https://pncp.gov.br/app/editais/26989715000102/2024/2508

SUPERIOR TRIBUNAL DE JUSTICA

Aquisição de solução de Detecção de Ameaças de Rede, composta de NDR e NPB, para permitir a detecção de atividades maliciosas na rede de dados, por meio de aprendizado de máquina, análise comportamental, entre outros mecanismos, serviços de instalação e configuração, com prestação contínua de suporte técnico e manutenção corretiva e evolutiva.

https://pncp.gov.br/app/editais/00488478000102/2024/531

PRODEB - CIA DE PROCESSAMENTO DE DADOS DA BAHIA

Contratação de empresa especializada para fornecimento de licença de atualização de novas assinaturas, patches, funcionalidades hospedadas na nuvem, suporte e garantia do fabricante da solução de segurança cibernética network detection and response ndr, do fabricante trend micro, para os sensores de proteção de rede, servidores e gerenciamento de risco da superfície de ataques deep discovery inspector (part number: ddnn0074), trend micro vision one - endpoint security (pro) (part number: vora0046) e trend vision one attack surface risk management asrm (part number: vona0000), pelo período de 24 (vinte e quatro) meses, conforme as especificações e condições estabelecidas no termo de referência.

Portal Nacional de Contratações Públicas

Conforme pode ser visto, no mercado há uma enorme quantidade de marcas e modelos de equipamentos de firewall, porém, para cada modelo e fabricante há necessidade de treinamento na configuração e implementação da solução, que a Prefeitura de Cariacica faz uso da solução do Fabricante Hillstone, que os técnicos em segurança da informação estão habituada às atividades do ambiente atual, o que trás redução na resolução de problemas comumente corriqueiros trazendo agilidade nas tarefas diárias do setor de segurança da informação.

A introdução de uma marca diferente implicaria em desafios como a necessidade de integração entre plataformas distintas (o que pode ser complexo e nem sempre eficiente), aumento da carga de gerenciamento, necessidade de novos treinamentos e potencial perda de sinergia operacional. Embora uma competição aberta pudesse, em tese, trazer preços menores para um equipamento isolado, os custos indiretos e os riscos associados à perda de padronização superam esse potencial benefício no contexto específico da Prefeitura de Cariacica.

Conforme posto, o mercado de Next-Generation Firewalls (NGFW) é composto por diversos fabricantes consolidados, cada fabricante oferece soluções com diferentes arquiteturas, funcionalidades e modelos de licenciamento. Uma análise completa de todas essas alternativas demandaria um esforço considerável e poderia não ser a mais eficiente dado o contexto da Prefeitura.

Conforme o Art. 41 e 43 da Lei nº 14.133/2021, é possível a indicação de marca em situações devidamente justificadas. Neste caso, a escolha pela continuidade da plataforma Hillstone se justifica tecnicamente e economicamente pelos seguintes motivos:

- **Padronização Tecnológica e Continuidade Operacional:** A Prefeitura já investiu em equipamentos Hillstone SG-6000-A5500 em 2024. A manutenção da mesma plataforma tecnológica é crucial para:
  - **Aproveitamento do Conhecimento Técnico (Curva de Aprendizagem):** A equipe da SUBTI já possui conhecimento e experiência na instalação, configuração, gerenciamento e troubleshooting dos firewalls Hillstone. A introdução de uma nova marca exigiria novo ciclo de treinamento, aumentando custos e o tempo necessário para que a equipe atinja proficiência, podendo impactar a agilidade na resposta a incidentes.
  - **Interoperabilidade e Integração:** A utilização de equipamentos do mesmo fabricante facilita a integração, o gerenciamento centralizado (por exemplo, com o Hillstone Security Management - HSM, se já utilizado ou planejado) e a aplicação de políticas de segurança consistentes em todo o ambiente. Isso reduz a complexidade da infraestrutura e minimiza riscos de incompatibilidade.
  - **Continuidade das Operações:** A familiaridade da equipe com a solução minimiza o risco de erros de configuração durante a implantação e manutenção, garantindo maior

estabilidade e disponibilidade dos serviços.

- **Justificativa Econômica:**
  - **Redução de Custos de Treinamento:** Elimina a necessidade de investir em capacitação para uma nova plataforma.
  - **Otimização de Custos Operacionais:** Um ambiente padronizado é mais simples de gerenciar, demandando menos tempo da equipe técnica e, potencialmente, reduzindo a necessidade de contratação de especialistas em múltiplas plataformas.
  - **Proteção do Investimento Anterior:** Maximiza o retorno sobre o investimento já realizado nos equipamentos Hillstone e no treinamento da equipe.
  - **Economia de Escala na Aquisição**: A aquisição de equipamentos e serviços do mesmo fornecedor pode resultar em melhores condições comerciais.

A aquisição dos Hillstone A5500 em 2023 foi motivada pela superioridade técnica em relação aos equipamentos anteriores. Presume-se que a solução tem atendido às expectativas de desempenho e segurança, justificando a continuidade.

ESTIMATIVA DO VALOR DA CONTRATAÇÃO

(art. 18 § 1º Inciso VI)

A estimativa precisa do valor da contratação será realizada na fase de elaboração do Termo de Referência, após pesquisa de preços junto a fornecedores e consulta a atas de registro de preços de outros órgãos públicos, conforme preconiza a legislação.

Foi realizada coleta prévia, porém, o valor final da pretendida aquisição, será aquele definido no instrumento Termo de Referência, caso o ETP seja aprovado.

Item	Descrição do item	Part Number	Unidade	Tipo do bem	Quantida Total	Previsão primeiro pedido	Valor unitário médio	Valor Total Unitário Médio	3STRUCTURE	WP COMPANY	SUPRISERVICE	ADD VALUE
1	Solução de Firewall de Controle de Aplicação	SG-6000-A5500-AD-IN60	HW	Permanente	4	2	R$ 670.225,00	R$ 2.680.900,00	R$ 718.000,00	633.000,00	R$ 628.900,00	R$ 701.000,00
2	Solução de Firewall de Perímetro	SG-6000-A3800-AD-IN60	HW	Permanente	4	2	R$ 330.595,00	R$ 1.322.380,00	R$ 350.500,00	330.000,00	R$ 321.500,00	R$ 320.380,00
3	Solução de Detecção e Resposta de Rede	BDS-IV08-SW-IN60	SW	Licença de uso	2	1	R$ 320.820,00	R$ 641.640,00	R$ 318.900,00	330.000,00	R$ 314.000,00	R$ 320.380,00
4	Solução de Detecção e Resposta Estendida	SG-6000-ISC6210-BP-IN	SW	Licença de uso	2	1	R$ 1.475.250,00	R$ 2.950.500,00	R$ 1.718.000,00	1.405.000,00	R$ 1.398.000,00	R$ 1.380.000,00
5	Solução de Balanceamento de Circuito	SG-6000-AX1200S-IN60	HW	Permanente	2	1	R$ 455.375,00	R$ 910.750,00	455.000,00	455.000,00	R$ 456.500,00	R$ 455.000,00

Item	Descrição do item	Part Number	Unidade	Tipo do bem	Quantidade Total	Previsão primeiro pedido	Valor unitário médio	Valor Total Unitário Médio	3STRUCTURE	WP COMPANY	SUPRISERVICE	ADD VALUE
6	Solução de Gerenciamento Centralizado de Firewall	SG-6000-vHSM-IN36	SW	Licença de uso	2	1	R$ 62.662,50	R$ 125.325,00	R$ 60.550,00	61.900,00	R$ 60.100,00	R$ 68.100,00
7	Solução de Centralização de Logs	SG-6000-VHSA-2-IN36	SW	Licença de uso	2	1	R$ 87.825,00	R$ 175.650,00	R$ 87.200,00	88.000,00	R$ 87.200,00	R$ 88.900,00
8	Solução Analítica de Rede	CloudV-Pro-5000	SW	Licença de uso	8	4	R$ 176.313,75	R$ 1.410.510,00	R$ 199.000,00	169.000,00	R$ 166.700,00	R$ 170.555,00
9	Treinamento para Solução de Firewall	N.A	SE	Treinamento	2	1	R$ 5.722,50	R$ 11.445,00	R$ 5.700,00	5.500,00	R$ 5.600,00	R$ 6.090,00
10	Treinamento para Solução de Detecção e Resposta de Rede	N.A	SE	Treinamento	2	1	R$ 5.722,50	R$ 11.445,00	R$ 5.700,00	5.500,00	R$ 5.600,00	R$ 6.090,00
11	Treinamento para Solução de Detecção e Resposta Estendida	N.A	SE	Treinamento	2	1	R$ 5.722,50	R$ 11.445,00	R$ 5.700,00	5.500,00	R$ 5.600,00	R$ 6.090,00
12	Treinamento para Solução de Balanceamento de Circuito	N.A	SE	Treinamento	2	1	R$ 5.722,50	R$ 11.445,00	R$ 5.700,00	5.500,00	R$ 5.600,00	R$ 6.090,00
13	Treinamento para Solução Centralização de Logs	N.A	SE	Treinamento	2	1	R$ 5.722,50	R$ 11.445,00	R$ 5.700,00	5.500,00	R$ 5.600,00	R$ 6.090,00
14	Treinamento para Solução	N.A	SE	Treinamento	2	1	R$ 5.722,50	R$ 11.445,00	R$ 5.700,00	5.500,00	R$ 5.600,00	R$ 6.090,00

Item	Descrição do item	Part Number	Unidade	Tipo do bem	Quantidade Total	Previsão primeiro pedido	Valor unitário médio	Valor Total Unitário Médio	3STRUCTURE	WP COMPANY	SUPRISERVICE	ADD VALUE
	Analítica de Rede											
15	Serviço de Operação Assistida da Solução de Segurança	N.A.	SE	Serviço	14	9	R$ 66.295,00	R$ 928.130,00	R$ 60.000,00	69.780,00	R$ 66.900,00	R$ 68.500,00
16	Serviço de Suporte Técnico 24x7	N.A.	CHAMADO	Serviço	200	100	R$ 5.922,50	R$ 1.184.500,00	R$ 6.000,00	6.000,00	R$ 5.600,00	R$ 6.090,00
17	Serviço de Suporte Técnico Especializado	N.A.	UST	Serviço	20	20	R$ 29.246,25	R$ 584.925,00	R$ 30.200,00	30.185,00	R$ 28.300,00	R$ 28.300,00
18	Instalação e Configuração de Firewall	N.A.	SE	Serviço	8	4	R$ 16.670,00	R$ 133.360,00	R$ 20.000,00	17.900,00	R$ 11.000,00	R$ 17.780,00
19	Instalação e Configuração de Solução de Detecção e Resposta de rede	N.A.	SE	Serviço	2	1	R$ 18.420,00	R$ 36.840,00	R$ 20.000,00	17.900,00	R$ 18.000,00	R$ 17.780,00
20	Instalação e Configuração de Solução de Detecção e Resposta Estendida	N.A.	SE	Serviço	2	1	R$ 18.420,00	R$ 36.840,00	R$ 20.000,00	17.900,00	R$ 18.000,00	R$ 17.780,00
21	Instalação e Configuração de Solução de Balanceamento de Circuito	N.A.	SE	Serviço	2	1	R$ 18.420,00	R$ 36.840,00	R$ 20.000,00	17.900,00	R$ 18.000,00	R$ 17.780,00

Item	Descrição do item	Part Number	Unidade	Tipo do bem	Quantidade Total	Previsão primeiro pedido	Valor unitário médio	Valor Total Unitário Médio	3STRUCTURE	WP COMPANY	SUPRISERVICE	ADD VALUE
22	Instalação e Configuração de Solução de Gerenciamento Centralizado de Firewall	N.A.	SE	Serviço	8	4	R$ 18.420,00	R$ 147.360,00	R$ 20.000,00	17.900,00	R$ 18.000,00	R$ 17.780,00
23	Instalação e Configuração de Solução de Centralização de Logs	N.A.	SE	Serviço	2	1	R$ 18.420,00	R$ 36.840,00	R$ 20.000,00	17.900,00	R$ 18.000,00	R$ 17.780,00
24	Configuração e Parametrização de Analítico de Rede	N.A.	SE	Serviço	2	1	R$ 18.420,00	R$ 36.840,00	R$ 20.000,00	17.900,00	R$ 18.000,00	R$ 17.780,00
							Total	**R$ 13.448.800,00**				

Nota: As quantidades e os modelos exatos dos equipamentos serão definidos no Termo de Referência**.**

Os valores acima indicados se tratam de uma expectativa inicial, que caso o presente instrumento seja aprovado, o Termo de Referência irá trazer de fato os valores reais e a expectativa de pedidos no ano corrente.

Que os valores citados acima tendem a uma aquisição parcial, mas de melhoria significativa ao conjunto dos serviços de segurança da informação desta Prefeitura; considerando se tratar de uma indicação de Registro de Preços, que a validade conforme a lei 14.133/21 é de 12 meses, podendo ainda ser prorrogado por mais 12 meses. Neste sentido, novos investimentos poderão ocorrer no ano de 2026 fazendo uso de recursos financeiros de outras Secretarias não mencionados neste documento.

Que a indicação do Plano Anual de Contratações de outras Secretarias poderá ser indicada a posteriori junto ao processo administrativo, cabendo às Secretarias indicadas caso a aprovação a sua apresentação junto aos autos do processo que conduzir este instrumento.

DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

(art. 18 § 1º Inciso VII)

Solução de Firewall Próxima Geração - Controle de Aplicação e Perímetro:

1. Deve ser capaz de operar no modo Camada 3 e Camada 2;
2. Características de NGFW, não utilizar UTM como referência;
3. Suporte a SNMP v1, v2 e v3;
4. Recursos avançados de NAT;
5. Limite de sessão com base no IP de origem, IP de destino, aplicação ou protocolo de aplicação;
6. Antivírus baseado em fluxo de rede;
7. Filtro Web baseado em fluxo;
8. Sandbox na Nuvem onde arquivos identificados como suspeitos/maliciosos para análise em ambiente computacional externo (cloud);
9. Identificar atividades de máquinas infectadas com sistemas de automação de tarefas (botnet) e C&C (Comando e Controle);
10. Filtrar o tráfego de endereços IPs de baixa reputação, incluindo Botnet, Spam;
11. Inspecionar o tráfego SSL/TLS;
12. Identificação de Windows, Linux, IOS, Android;
13. Controle de largura de banda em um endereço IP ou usuário;
14. Operar nos modos Ativo/Ativo e Ativo/Passivo;
15. Exportar Syslog padrão;
16. Estatísticas de tráfego em “tempo real”;
17. Estatísticas de eventos de segurança;

NDR (Network Detection and Response):

1. Deve ser fornecido equipamento como appliance virtual;

2. Ter mecanismos de análise comportamental, baseada em aprendizado de máquina (machine learning
3. Análise de correlação de ameaças desconhecidas, comportamento anormal e comportamento de aplicações
4. Metodologia de classificação de ameaças seguindo critérios de risco
5. Detecção de malware baseada em comportamento;
6. Detecção de DDOS
7. Inspeção do tráfego de túneis criptografados
8. Suportar captura online de pacotes
9. Exibição de ameaças de “intranet/internet”
10. Operação com espelhamento de porta
11. Identificar aplicações em nuvem
12. Identificar atividades de máquinas infectadas com botnet;
13. Envio de arquivos identificados como suspeitos/maliciosos para análise em ambiente computacional externo (cloud);
14. Recurso de armadilhas (honeypot) locais

XDR (Extended Detection and Response):

1. Visualização de ativos de risco e tendências de risco;
2. Tela cheia de informações detalhadas e estatísticas para segurança
3. Análise do comportamento
4. Análise de correlação
5. Estatísticas e análises sobre risco
6. Coleta de evidências
7. Gerenciamento de ativos
8. Descoberta automática de ativos
9. Estatísticas e detalhadas sobre vulnerabilidades
10. Integração com scanners de terceiros
11. Banco de dados de inteligência de domínios dns, códigos maliciosos, ip, vulnerabilidades, detecção de intrusão e geolocalização
12. Análise de correlação de big data e detecção de killchain
13. Pesquisa centralizada e classificada para eventos
14. Recurso de sistema de gerenciamento de casos
15. Capacidade de criação de playbooks
16. Possuir suporte a políticas entregues ao firewall
17. Segurança de endpoint
18. Segurança do servidor

19. De resposta a incidentes
20. Função opcional da tarefa de relatório

ADC (Application Delivery Controller):

1. Deve ser um equipamento físico;
2. Possuir balanceamento de carga de servidores (SLB)
3. Possuir balanceamento global de carga de servidores (GSLB)
4. Recursos para melhorias de performance
5. Deve suportar a identificação de aplicações com base no comportamento e nas características da aplicação.

NIPS (Network Intrusion Prevention System):

1. Deve ser um equipamento físico;
2. Possui base de aplicações que podem ser filtradas por nome, categoria, subcategoria, tecnologia e risco.
3. Identificação da aplicação para tráfego criptografado SSL
4. Prevenção de intrusões para o tráfego criptografado SSL.
5. proteção do ambiente IPv6.
6. proteção contra ataques de injeção SQL, CC e XSS.
7. modo de operação de sniffer IDS.
8. Criação de assinaturas IPS definidas pelo usuário.
9. Detecção de reputação IP e o bloqueio de IP e Banco de Dados de Reputação IP Global.
10. Detectar de anomalia de protocolo
11. A solução deve suportar o Antivírus baseado em fluxo
12. Proteger efetivamente contra bots de intranet e evitar novos ataques de ameaças avançadas
13. Classificar e prevenir spam em tempo real.

Solução de Gerenciamento Centralizado de Firewall:

1. Edição da mesma política de segurança por mais de um usuário administrador de forma simultânea;
2. Interface única de gerência dos equipamentos a suas configurações de rede, de segurança, gerência de logs, geração de relatórios e sistema de gerência de tráfego WAN;
3. Permitir definir regras (política de segurança), sobre as quais todas as demais regras ficarão subordinadas;
4. Gerenciamento centralizado das licenças dos equipamentos monitorados;
5. Localização de regras em que determinado endereço IP, range de IP, sub- rede ou objeto;
6. Atualização dos firewalls de forma remota;

7. Gerenciamento de todos os equipamentos em uma console única de gerenciamento.

Centralizador de LOGs:

1. Appliance virtual
2. Armazenamento em disco para diferentes tipos de log;
3. Estado de dispositivos que enviam logs;
4. Consultas personalizadas ou filtro de condições;
5. Log de eventos, log de rede, log de configuração, log IPS;
6. Log de sessão ipv6, log NAT, log PBR, log SLB;
7. A logs do Windows;
8. Suporte a consultas de tarefas em segundo plano;
9. Suporte para análise, armazenamento e exibição dos novos logs de Firewall;
10. Backup de logs para ambiente externo através de FTP e SFTP;

Analítico de Rede (Network Analytics):

1. O serviço de segurança baseado em nuvem;
2. Classificação das principais aplicações por uso do tráfego;
3. Apresentar os eventos de ameaça e permitir a verificação de detalhes das ameaças;
4. Possuir suportar classificação de principais ameaças com base no nome da ameaça;
5. Criação de regra de alarme;
6. Enviar alarmes via e-mail;
7. Apresentar as estatísticas do tráfego do sistema e detecção de anomalias no tráfego;
8. Monitor centralizado para vários dispositivos;

Solução de Microsegmentação:

1. Controle granular de nível de nó ou aplicativo para
2. Política de Microsegmentação
3. Simulação de política de Microsegmentação
4. Regras de comportamento para hosts,
5. Serviços de monitoramento de comportamento
6. Verificação de conformidade do arquivo de configuração manual para imagens docker e clusters kubernetes
7. Varredura de vulnerabilidades;
8.

Solução de Proteção de Máquina virtual:

1. Descoberta de Redes e VMs;
2. Visualização de topologia de rede, VM e Tráfego, na intranet e internet;

3. Agrupamento de VMs por Controle de Acesso; 4. Atuar nas camadas de rede de 4 a 7;
Treinamento 1. O treinamento deve ser previsto para todas as ferramentas, bem como contemplar integração entre as soluções.
Suporte e Operação 1. Deve ser previsto suporte técnico e garantia do Fabricante da Solução em toda a vigência contratual, sendo emitida Documentação do fabricante que garanta o fornecimento desses serviços. **2.** Deve ser previsto suporte especialista para a Operação das Soluções.

JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

(art. 18 § 1º Inciso VIII)

Conforme pode ser verificado junto ao presente documento, um Lote Único atende aos níveis de complexidade e integração das Soluções, em sua administração e necessitam de atenção priorizada em relação às camadas de segurança que representam, nesse caso, consideramos também, estar de acordo com a redução de custos de gestão de contratos e ainda com a economia de escala, definindo mantê-los em um único lote.

A regra geral de parcelamento do objeto deve ser coordenada com o requisito da viabilidade técnica para sua adoção. Não se imagina viável quando o objeto é fisicamente único. Nesse sentido, um exame atento dos tipos de objeto licitados pela Administração Pública evidência que embora sejam divisíveis, em tese, há interesse técnico na manutenção da unicidade da licitação ou do item da mesma. Não é, pois, a simples divisibilidade, mas a viabilidade técnica que dirige o processo decisório. Observa-se que, na aplicação dessa norma, até pela disposição dos requisitos fisicamente dispostos no seu conteúdo, à avaliação sob o aspecto técnico precede a avaliação sob o aspecto econômico.

Lei 14.133/2021:

Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

§ 3º O parcelamento não será adotado quando:

I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;
II - o objeto a ser contratado configurará sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido.

Se um objeto, divisível, sob o aspecto econômico for mais vantajoso, mas houver inviabilidade técnica em que seja licitado em separado, de nada valerá a avaliação econômica. Imagine-se ainda considerando a aquisição dos serviços e equipamentos fossem realizados isoladamente e custasse mais barato, mesmo assim seria recomendável o não parcelamento deste projeto, pois sob o aspecto técnico é a visão do conjunto que iria definir a garantia total do fabricante com reposição de componentes danificados ou relançamento de alguma parte do cabeamento óptico rompido, partes que tornam orgânico e harmônico todo o objeto. Em outros termos, de nada adianta eventual vantajosidade econômica, em termos absolutos, se o produto for imprestável para a finalidade que se pretende alcançar.

É importante ressaltar, ainda, que o objeto contratado somente tem utilidade para a administração pública se todos os itens estiverem em pleno funcionamento. Se houver a divisão em lotes e, por alguma razão, um lote não for entregue ou não estiver em funcionamento, todo o resto da contratação não terá utilidade alguma para a Administração, ocasionando prejuízos milionários.

Pode-se concluir, pelo princípio da finalidade, um dos princípios básicos da Administração Pública, que a aquisição na forma aqui proposta traz mais vantagens e benefícios para a Administração e garantia de melhores condições para a realização do serviço, com qualidade e sem sofrer solução de continuidade.

Nessa situação haverá nítida desoneração burocrática; diminuição do risco de desorganização; maior possibilidade de se atingir o fim almejado; redução do comprometimento operacional; e, consequentemente, possibilidade de êxito em sua realização.

Por esses motivos, conclui-se pela aquisição em um único lote, respeitando a integridade qualitativa do objeto a ser executado, mantendo a unidade do objeto em respeito à viabilidade técnica.

Os bens/serviços a serem adquiridos/contratados são comuns, pois têm especificações usuais, caracterizando-se por padrões de desempenho e qualidade que podem ser objetivamente definidos e entendidos pelo mercado.

Ressalta-se que o agrupamento dos itens em um único lote se deve ao fato de que todos os bens e serviços a serem contratados estão intrinsecamente relacionados (uma única solução); além disso, todos os equipamentos serão gerenciados de forma centralizada. O fornecimento de tais itens por mais de uma empresa certamente tornaria o projeto inviável, já que acarretaria elevado custo de administração e uma complexa rede de coordenação de diversos contratos com o mesmo objeto; o que, certamente, não encontra amparo legal, além de comprometer a qualidade e efetividade dos resultados para a Contratante**.**

DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS, EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS DISPONÍVEIS

(art. 18 § 1º Inciso IX)

Resultados Pretendidos:

- ***Segurança Aprimorada:*** *Elevação do nível de proteção contra ameaças cibernéticas avançadas, reduzindo o risco de incidentes de segurança, vazamento de dados e interrupção de serviços.*
- ***Melhoria de Desempenho e Disponibilidade:*** *Maior capacidade de processamento de tráfego, garantindo a performance das aplicações e a disponibilidade dos serviços para cidadãos e servidores.*
- ***Conformidade Legal:*** *Auxílio no cumprimento de requisitos da LGPD e outras normativas relacionadas à segurança da informação.*
- ***Visibilidade e Controle:*** *Melhor capacidade de monitoramento do tráfego de rede e controle sobre as aplicações utilizadas.*

- ***Economicidade:***
  - *Prevenção de custos associados a incidentes de segurança (multas, recuperação de dados, danos à imagem).*
  - *Redução de custos operacionais a longo prazo devido à padronização (menor necessidade de treinamento em múltiplas plataformas, gerenciamento simplificado).*
  - *Potencial para melhores condições comerciais na aquisição de uma solução padronizada e pela modalidade de ARP.*

- ***Melhor Aproveitamento dos Recursos:***
  - ***Recursos Humanos:*** *A equipe técnica da SUBTI poderá focar em atividades mais estratégicas, uma vez que o gerenciamento de uma plataforma padronizada e familiar é mais eficiente. O conhecimento adquirido é potencializado.*

- ***Recursos Materiais:*** *Maximização do uso da infraestrutura de TI existente, garantindo que os investimentos em segurança acompanhem a evolução das necessidades.*
- ***Recursos Financeiros:*** *Aplicação mais eficiente dos recursos públicos, direcionando investimentos para uma solução que oferece o melhor equilíbrio entre custo, benefício, risco e alinhamento estratégico com os ativos existentes.*

PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

(art. 18 § 1º Inciso X)

- *Elaboração do Termo de Referência detalhado, com as especificações técnicas finais, quantidades precisas e níveis de serviço.*
- *Realização de ampla pesquisa de mercado para composição do preço estimado da contratação para a Ata de Registro de Preços.*
- *Designação do gestor e fiscais do contrato, que deverão ter conhecimento técnico sobre soluções de firewall e gestão de contratos de TI. A equipe da SUBTI já possui familiaridade com a solução Hillstone, o que facilita esta etapa.*
- *Verificação da infraestrutura física (espaço em rack, pontos de energia e refrigeração) nos locais onde os novos equipamentos serão instalados.*
- *Planejamento da janela de instalação e migração para minimizar o impacto nos serviços da Prefeitura.*
- *Garantia da disponibilidade orçamentária para a adesão à Ata de Registro de Preços, conforme planejamento para o PAC 2026.*

CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

(art. 18 § 1º Inciso XI)

Não serão necessárias contratações correlatas para a pretensa aquisição.

DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS, INCLUÍDOS REQUISITOS DE BAIXO CONSUMO DE ENERGIA E DE OUTROS RECURSOS, BEM COMO LOGÍSTICA REVERSA PARA DESFAZIMENTO E RECICLAGEM DE BENS E REFUGOS, QUANDO APLICÁVEL

(art. 18 § 1º Inciso XII)

O objeto desta contratação, pelo alto nível de tecnologia embarcada em seus processos de fabricação e integração das diversas tecnologias empregadas demandam uma expertise que poucas empresas dominam e, pelo nicho em que operam, necessitam atender a políticas de qualidade e certificações voltadas para a governança ambiental e sustentabilidade, sob pena de sanções e consequentemente, perda de mercado.
Isto posto, a contratação ora pretendida prevê a aquisição de racks inteligentes para instalação em ambiente interno, sendo desnecessária qualquer intervenção no meio ambiente, portanto conclui-se que não há impactos ambientais relevantes relacionados à pretensa contratação.

POSICIONAMENTO CONCLUSIVO DO MODELO DA SOLUÇÃO DE TI A SER CONTRATADA

(art. 18 § 1º Inciso XIII)

Para garantir Governança, Gestão Tática e Operacional de alto nível em Segurança da Informação e Cibernética, a utilização da solução apresentada torna-se a opção mais viável objetivando garantir a proteção dos ativos da informação, tendo em vista que a PMC, atualmente, tem efetuado uma grande modernização com utilização híbrida de Serviços hospedados interna e externamente.

Considerando o exposto acima, bem como, os estudos e pesquisas junto às tecnologias disponíveis no mercado, realizados pela Gerência de Segurança da Informação, entendemos ser necessário a aquisição de uma Modernização da Segurança Cibernética e Privacidade de Dados, para ampliar o monitoramento e resposta a incidentes, bem como proteger os Ativos da Informação da Prefeitura, tendo em vista o crescimento tecnológico previsto para os próximos anos por meio dos investimentos da atual Gestão.

RESPONSÁVEIS PELA ELABORAÇÃO E APROVAÇÃO

(art. 18 § 1º Inciso XIII)

Cariacica, 04 de junho de 2025.

Elaboração:

Nome: Antônio Carpanedo Fiório
Cargo: Gerente de Contratações de Tecnologia da Informação
Setor: Subsecretaria de Tecnologia da Informação (SUBTI)

Aprovação:

Nome: Nilson Callegari Teixeira
Cargo: Subsecretário de Tecnologia da Informação
Setor: Subsecretaria de Tecnologia da Informação - SEMFI/SUB-TI

ANEXO I

ANÁLISE E MAPEAMENTO DOS RISCOS DA CONTRATAÇÃO

RISCO 1			
Descrição: Deficiência na definição da demanda			
Probabilidade:	(X) Pouco	( ) Provável	( ) Muito
Impacto:	( ) Baixo	( ) Médio	(X) Alto
Fase Impactada:	( ) Fase Interna	( ) Fase Externa	(X) Gestão do Contrato
Id	**Dano**		
1.	Superdimensionamento ou subdimensionamento da demanda		
Id	**Ação Preventiva**		**Responsável**
1.	Qualificação da equipe de planejamento; conhecimento do escopo.		Setor Demandante
Id	**Ação de Contingência**		**Responsável**
1.	Revisão do projeto de restabelecimento da demanda.		Equipe de Planejamento da Contratação

RISCO 2			
Descrição: Não aprovação do Estudo Técnico ou do Termo de Referência.			
Probabilidade:	(X) Pouco	( ) Provável	( ) Muito
Impacto:	( ) Baixo	(X) Médio	( ) Alto
Fase Impactada:	(X) Fase Interna	( ) Fase Externa	( ) Gestão do Contrato
Id	Dano		
1.	Atraso no processo de contratação e, consequentemente, atraso no início da prestação do serviço.		
Id	**Ação Preventiva**		**Responsável**
1.	Instruir o Estudo Técnico e o Termo de Referência em estrita aderência às disposições dos normativos aplicados à contratação.		Equipe de Planejamento da Contratação
Id	**Ação de Contingência**		**Responsável**
1.	Exposição do arcabouço legal em que a contratação de serviços de limpeza deva seguir.		Equipe de Planejamento da Contratação

ANEXO II

MATRIZ DE ALOCAÇÃO DE RISCOS DO CONTRATO

RISCO 1			
Descrição: Inércia frente a descumprimento de obrigações contratuais. Falha ou omissão no registro dos atos e fatos do contrato.			
Probabilidade:	(X) Pouco	( ) Provável	( ) Muito
Impacto:	( ) Baixo	(X) Médio	( ) Alto
Id	Materialização		
1.	Deficiência na prestação dos serviços. Prejuízos financeiros a Administração		
Id	**Ação de mitigação**		**Alocação**
1.	Capacitação de servidores; Conhecimento dos termos contratuais e do serviço a ser executado. Conhecimentos das responsabilidades dos fiscais. Estabelecer modelos e rotinas de acompanhamento contratual		Fiscal técnico e administrativo, Gestor do Contrato

RISCO 2			
Descrição: Descumprimento das obrigações trabalhistas, previdenciárias e com FGTS da Contratada.			
Probabilidade:	(X) Pouco	( ) Provável	( ) Muito
Impacto:	(X) Baixo	( ) Médio	( ) Alto
Id	Materialização		
1.	Responsabilização subsidiária da Administração		
Id	**Ação de mitigação**		**Alocação**
1.	Capacitação de servidores; Previsão expressa no termo de contrato. Conhecimento dos termos contratuais. Conhecimentos das responsabilidades dos fiscais. Estabelecer modelos e rotinas de acompanhamento contratual		Fiscal técnico e administrativo, Gestor do Contrato.

RISCO 3			
Descrição: Atraso nas entregas e descumprimento de prazos.			
Probabilidade:	( ) Pouco	(X) Provável	( ) Muito
Impacto:	( ) Baixo	(X) Médio	( ) Alto
Id	Materialização		

1.	Atraso no início e consequentemente na finalização do projeto	
Id	**Ação de mitigação**	**Alocação**
1.	Acompanhamento dos prazos previstos, bem como desenvolver cronograma de entrega prevendo possíveis atrasos, de modo a não haver comprometimento das entregas	Fiscal técnico e administrativo, Gestor do Contrato.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi assinado eletronicamente e pode ser acessado no endereço https://sei.cariacica.es.gov.br/autenticidade utilizando o identificador 350034003600310030003900 3A00540052004100

Assinado eletronicamente por **ANTONIO CARPANEDO FIORIO** em **04/06/2025 15:36**
Checksum: **E543595D41E6D57D0928B1836DF3800DB9CDBF4B52385F3F7D30E84CAA04C977**

Assinado eletronicamente por **NILSON CALLEGARI TEIXEIRA** em **04/06/2025 16:11**
Checksum: **29BFE90ADD5809E21799237BB841EA2FA6332DCA3C48F09C74993B4A79E38814**