



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

ESTUDO TÉCNICO PRELIMINAR

PROCESSO DIGITAL nº 357 / 2025

**Solução de Microsegmentação com serviços de
implantação, suporte técnico, manutenção,
treinamento e horas de projeto sob demanda.**

Versão: 1.0 – Novembro/2025

São Paulo, 25 de Novembro de 2025



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

1. INTRODUÇÃO

O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação.

O ETP tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização da Demanda – DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação.

Referência: Inciso XI, do art. 2º e art. 11 da IN SGD/ME nº 94/2022.

2. NECESSIDADE DA CONTRATAÇÃO

A atual arquitetura de rede da Alesp segue um modelo tradicional de segmentação baseado em VLANs, sub-redes e ACLs aplicadas em roteadores e switches. Embora este modelo seja suficiente para organizar a rede em grandes blocos funcionais (como por tipo de serviço ou departamento), ele é limitado em termos de granularidade, automação, escalabilidade e, principalmente, segurança contra ameaças laterais, característica marcante de ataques modernos, como ransomwares e ameaças persistentes avançadas.

A ausência de um mecanismo de controle de acesso entre cargas de trabalho, usuários e dispositivos no nível mais granular da rede (por exemplo, entre máquinas virtuais, containers, servidores ou mesmo dispositivos IoT) abre caminho para que um atacante que comprometa um único ativo tenha liberdade para se mover lateralmente pela rede, acessando dados, sistemas e serviços críticos. Este tipo de movimento é notoriamente difícil de detectar com tecnologias convencionais, como firewalls de perímetro ou segmentações tradicionais.

Além disso, o modelo atual de segurança depende fortemente de regras estáticas e intervenção manual, o que dificulta a resposta rápida a incidentes e torna a política de segurança propensa a falhas de configuração. A falta de visibilidade em tempo real sobre as comunicações leste-oeste (intra-rede) também compromete a capacidade de investigação e correção em caso de incidentes.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

A microssegmentação é uma abordagem de segurança baseada em software que permite a definição e aplicação de políticas de segurança em nível de aplicação ou carga de trabalho, independentemente da infraestrutura física subjacente. A solução promove:

- Isolamento de serviços críticos;
- Restrição do tráfego lateral com base em identidade, função ou contexto de segurança;
- Automação de políticas dinâmicas integradas com fontes de identidade (ex.: AD, LDAP, MDM);
- Detecção e contenção automática de comportamentos anômalos;
- Mapeamento detalhado das dependências de rede e fluxos de comunicação.

Estudos recentes e casos de ataque como os observados com malwares do tipo ransomware demonstram que a falta de controles de microvisibilidade e segmentação contribui diretamente para o impacto dos ataques, permitindo a criptação de ativos fora do escopo do comprometimento inicial.

Além do risco cibernético, há desafios de conformidade e governança. A ausência de uma arquitetura de segurança segmentada torna difícil a implementação de boas práticas de segurança como políticas de acesso de privilégio mínimo, por exemplo, preconizadas por frameworks como *NIST SP 800-207 - Zero Trust Architecture (ZTA)*.

Adicionalmente, o parque tecnológico da instituição é heterogêneo, com equipamentos de múltiplos fabricantes e diferentes níveis de suporte a políticas de segurança nativas. Isso reforça a necessidade de uma solução independente de hardware, que permita controle uniforme e centralizado da política de segurança.

Por fim, a adoção de microssegmentação encontra aderência aos objetivos estratégicos e regulatórios expressos, por exemplo, no ATO DE MESA Nº 3, DE 03 DE FEVEREIRO DE 2022, em especial nos seguintes pontos:

Art. 4º - São princípios da PSI:

V - a contínua análise dos riscos aos quais a informação está sujeita, considerando também aspectos da cultura organizacional da ALESP;

VI - a incorporação da segurança como requisito essencial dos sistemas de informação, informatizados ou não;

Art. 5º - Com vistas à observância aos princípios descritos no artigo 4º deste Ato, a PSI está voltada aos seguintes objetivos:

II - implantar a contínua avaliação dos riscos a que a informação está sujeita, incluindo, mas não se limitando, a medição de indicadores quantificáveis;

III - estabelecer mecanismos que visem garantir a segurança da informação, em especial a confidencialidade, a integridade, a disponibilidade e a autenticidade nos projetos, processos e atividades da ALESP;



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

Art. 6º - São diretrizes da PSI:

IV - observância de leis, regulamentos e obrigações contratuais aos quais os processos de trabalho estão sujeitos, bem como as normas e boas práticas, aplicáveis.

Art. 14 - As demandas iniciais do CGSI às unidades administrativas da ALESP competentes para elaboração e revisão de normas e procedimentos relativos à segurança da informação terão como prioridade os seguintes temas, sem prejuízo de eventuais necessidades prementes:

I - acesso, proteção e guarda da informação, em especial a informação sigilosa e a informação pessoal;

II - aquisição, desenvolvimento e manutenção de sistemas informatizados;

III - autenticação e controle de acesso à rede de dados, aos serviços de tecnologia da informação e comunicação e aos sistemas de informação da ALESP;

V - coleta e preservação de registros de segurança;

VII - gestão de incidentes de segurança da informação;

VIII - inventário dos recursos computacionais e dos conteúdos informacionais, em consonância com o Programa de Gestão de Documentos da Assembleia Legislativa instituído pelo Ato da Mesa nº 2, de 1º de março de 2013, enfatizando os aspectos de responsabilidades e de uso aceitável;

IX - Plano de Continuidade de Negócio;

X - segregação de ambientes de tecnologia da informação e comunicação, com a implementação de ambientes distintos de desenvolvimento, teste, homologação e produção de sistemas computacionais, feita em atendimento ao princípio da separação de funções, com a definição de papéis e responsabilidades específicos para cada ambiente;

XI - segurança das instalações que hospedam os conteúdos informacionais e os recursos computacionais para os quais a normatização seja necessária.

Portanto, a contratação de uma solução de microssegmentação de rede não apenas atende às demandas técnicas de segurança e gestão modernas, como também está alinhada às diretrizes institucionais de governança e conformidade, sendo medida imprescindível para a evolução da maturidade cibernética da Alesp.

Ressalta-se ainda que o objeto da contratação **não consta no Catálogo Eletrônico de Padronização** (<https://www.gov.br/pncp/pt-br/catalogo-eletronico-de-padronizacao>, acessado em 11/11/2025).

3. PREVISÃO NO PLANO DE CONTRATAÇÃO ANUAL - PCA

A Alesp não tem Plano de Contratações vigente para o ano de 2025.



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

4. REQUISITOS DA CONTRATAÇÃO

4.1. Condições Gerais

- 4.1.1.** A CONTRATADA deverá respeitar integralmente as normas de segurança estabelecidas pela ALESP e atender aos padrões de segurança e controle para acesso e uso das instalações e equipamentos da ALESP, zelando por sua integridade.
- 4.1.2.** A CONTRATADA obriga-se por si, seus empregados, sócios, diretores e mandatários, a manter total sigilo e confidencialidade dos serviços prestados à ALESP no que se refere a não divulgação, por qualquer forma, no todo ou parte das informações e/ou documentos a ele relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados por força deste contrato, com vistas à Lei 13.709/2018 (Lei Geral de Proteção de Dados).
- 4.1.3.** O valor de pagamento e o devido cronograma de faturamento devem seguir os respectivos Cronogramas Físico-Financeiros, apresentados no Anexo I deste Termo de Referência, respeitando a porcentagem definida.
- 4.1.4.** É vedada a subcontratação do objeto desta licitação.

4.2. Sustentabilidade

- 4.2.1.** Por se tratar de solução em formato de appliance virtual, a contratação contribui para a sustentabilidade, na medida em que evita a aquisição de novos equipamentos físicos, reduzindo o consumo de energia elétrica, a utilização de materiais para fabricação de hardware e a geração futura de resíduos eletrônicos.

4.3. Solução de Microsegmentação para Servidores (ITEM 2)

4.3.1. Especificações Gerais da Solução

- 4.3.1.1.** A solução tecnológica deverá ser entregue em modelo SaaS, implantada em nuvem e hospedada pela CONTRATADA e totalmente dedicada para a CONTRATANTE, podendo também ser implantada em modelo On-Premises no data center da CONTRATANTE, com garantia e suporte da licença pelo período de 24 meses. O uso em SaaS não requer componentes locais, exceto pelos agentes instalados nos ativos protegidos.



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

- 4.3.1.2.** A solução ofertada deverá existir como produto pronto antes do lançamento do edital, não sendo aceitos produtos em fase alfa, beta ou qualquer fase anterior à versão final e estável;
- 4.3.1.3.** O período de garantia das licenças deverá começar a contar a partir da data de instalação e ativação no ambiente da ALESP, prevista na Etapa 2 da Fase 1 do Modelo de Execução do Objeto, que ocorre somente após a entrega e aprovação do Plano de Implantação (Etapa 1 da Fase 1).
- 4.3.1.4.** A solução deverá ser compatível com VMware vSphere Hypervisor (ESXi) 7.0.3 e versões superiores. Não será necessário fornecer equipamentos ou licenças para virtualização da solução.
- 4.3.1.5.** Todos os itens da solução devem ser de mesmo fabricante, para garantir total integração.
- 4.3.1.6.** Não serão aceitas soluções de código livre ou open source.
- 4.3.1.7.** A solução deverá suportar a criação de grupos de usuários que permitam a administração baseada em diferentes perfis de acesso às configurações do sistema (leitura/escrita, só leitura).
- 4.3.1.8.** A solução ofertada deverá ser um produto final, estável e oficialmente lançado pelo fabricante antes da data de publicação deste edital, não sendo aceitos produtos em fase alfa, beta, piloto ou qualquer versão preliminar.
- 4.3.1.9.** A solução SaaS deverá estar hospedada primariamente em Datacenter localizado em território brasileiro, podendo utilizar outro país como contingência;
- 4.3.1.10.** Componentes administrativos da solução não deverão possuir dependência de nenhum outro componente de rede ou infraestrutura para o seu perfeito funcionamento.
- 4.3.1.11.** A solução deve prover no mínimo 99.5% de disponibilidade no nível de serviço;
- 4.3.1.12.** Deve suportar a microsegmentação tanto em dispositivos físicos quanto em dispositivos virtualizados.
- 4.3.1.13.** Deverá suportar configuração em modo de Alta Disponibilidade (HA) e Redundância de instâncias e serviços e, em caso de indisponibilidade



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

da instancia ativa, o serviço deverá ser automaticamente migrado, sem prejuízo para a prestação dos serviços.

- 4.3.1.14.** Deverá garantir a sincronização das bases entre as instancias, de modo a viabilizar a recuperação de desastres, sem prejuízo para os serviços.
- 4.3.1.15.** O sistema deve adotar o Controle de Acesso Baseado em Função (RBAC). Esta funcionalidade deve assegurar que cada usuário tenha apenas as permissões essenciais para sua atividade, aplicando o princípio do menor privilégio. O controle de acesso deve ser granular, baseado em papéis (roles) e escopos (scopes), permitindo também a criação de perfis personalizados.
- 4.3.1.16.** Deverá utilizar métodos de propagação e sincronização de alterações de dados em tempo real e de forma criptografada.
- 4.3.1.17.** Deverá permitir que, durante o processo de atualização de software, a solução não sofra qualquer interrupção de serviço.
- 4.3.1.18.** Deverá prover auditoria de logs de todas as ações e mudanças realizadas na solução.
- 4.3.1.19.** Deverá fornecer mecanismos para recuperação rápida de configurações através da interface de gerenciamento web.
- 4.3.1.20.** Deverá possuir capacidade de reverter configurações sem a necessidade de restauração de backup.
- 4.3.1.21.** Deverá prover conjunto de integrações que permitam automação e resposta de orquestração de segurança (SOAR) e melhorar todo o ecossistema de segurança cibernética por meio de automação aprimorada e compartilhamento de dados bidirecional em tempo real em todo o ecossistema, habilitado por APIs ou conexões nativas.
- 4.3.1.22.** Para garantir a segurança dos dados desta organização, o ambiente em nuvem deverá ser dedicado para este órgão. Nenhuma informação deverá ser compartilhada, incluindo os IPs e FQDNs de acesso da Console de Gerenciamento, bem como de todos os outros componentes na nuvem do fabricante da solução;
- 4.3.1.23.** A solução deverá utilizar agentes instalados nos ativos protegidos, responsável por coletar os fluxos de dados e garantir a aplicabilidade das regras configuradas;



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

- 4.3.1.24.** A comunicação entre o agente e a console central deve ser criptografada.
- 4.3.1.25.** Deve ser capaz de ser implantado em vários segmentos de rede (VLANs), independente do equipamento utilizado para controlar a VLAN;
- 4.3.1.26.** A solução deverá possuir a capacidade de Etiquetamento de todos os ativos, incluindo os que possuem agentes ou outros ativos sem agente mas que se comunicaram ou receberam comunicação de um ativo protegido pela solução;
- 4.3.1.27.** Deverá também estar licenciado para todos os servidores que estão no objeto desta contratação, inclusive para o HA (cluster de alta disponibilidade) da console.
- 4.3.1.28.** Deve possibilitar a criação de ilhas no ambiente, onde os ativos tenham sua comunicação restrita apenas ao que for previamente identificado e liberado.
- 4.3.1.29.** Deverá suportar a segmentação de ambientes em contêineres, minimamente ambientes Kubernetes, OpenShift, Rancher e Docker. É desejável também suporte a outros tipos de ambientes em contêineres como EKS, AKS, Containerd, CRI-O, Calico, Flannel, etc..
- 4.3.1.30.** A solução deve possuir, no mínimo, conectores para as seguintes nuvens públicas: AWS, Azure, GCP, Oracle Cloud; e também VMware vSphere, LDAP/LDAPS, MS Active Directory, F5, OpenStack.
- 4.3.1.31.** Deverá prover API Rest para inclusão, alteração, exclusão ou consulta de objetos;
- 4.3.1.32.** As operações citadas acima devem fornecer alternativas para execução em lote, com mecanismo para garantir que tais alterações não irão gerar impactos nos serviços em produção.
- 4.3.1.33.** Deverá possuir logs de tráfego e eventos com retenção local por, pelo menos, 90 dias com mecanismos de pesquisa e filtros com possibilidade de integração com SIEM para análise de eventos e estatística de logs.
- 4.3.1.34.** Deverá fornecer dados estatísticos e métricas sobre nível de utilização e funcionalidades do sistema como um todo.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- 4.3.1.35.** A solução deverá possuir rotinas de gravação de logs detalhados de todas as operações de manutenção do sistema, incluindo a identificação do usuário responsável, com retenção mínima de 30 (trinta) dias.
- 4.3.1.36.** A solução deverá permitir integração nativa com servidores Syslog, possibilitando o envio de todos os logs de auditoria, eventos e operações para sistemas de gestão e monitoramento externos.
- 4.3.1.37.** A solução deverá ser dimensionada de forma a atender um ambiente com as seguintes características:

Tipo de Ativo	Qtd
Servidores Físicos "Bare metal"	10
Máquinas Virtuais "Virtual Machines"	260
Contêineres "Containers"	80
Desktops	1.850
Notebooks	300
TOTAL	2.500

4.3.2. Console de Gerenciamento

- 4.3.2.1.** A solução deverá disponibilizar console administrativa baseada em navegador, acessível via protocolo HTTPS.
- 4.3.2.2.** A solução deverá oferecer interface Web para usuário compatível, no mínimo, com os navegadores Google Chrome e Mozilla Firefox, em suas versões atuais.
- 4.3.2.3.** O console deve permitir controle de acesso baseado em funções (RBAC), possibilitando perfis diferenciados de usuários com permissões específicas para configuração, monitoramento e auditoria.
- 4.3.2.4.** Todas as ações administrativas, alterações de políticas, acessos e eventos relevantes devem ser registradas em logs auditáveis, com possibilidade de exportação em formato compatível para análise externa.
- 4.3.2.5.** A interface deverá oferecer dashboards personalizáveis para visualização de métricas, fluxos de tráfego e status de políticas em tempo real, permitindo acompanhamento operacional detalhado.
- 4.3.2.6.** Deve possuir auditoria para rastreamento de todas as modificações realizadas na console administrativa.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- 4.3.2.7.** Deve permitir integração via SAML 2.0 e OAuth com IdPs externos como, no mínimo o Micro Focus/NetIQ Identity Manager (IDM) + NetIQ Access Manager (NAM) e Microsoft Azure AD\Entra, possibilitando autenticação na console administrativa a partir de um usuário gerenciado internamente pela CONTRATANTE.
- 4.3.2.8.** A console de gerenciamento deverá ser única para toda a solução de micro segmentação;
- 4.3.2.9.** Ter a capacidade de gerenciar todos os tipos de ativos em uma única console;
- 4.3.2.10.** Ter a capacidade de visualizar os fluxos de dados e configurar as políticas de segurança em uma única console;
- 4.3.2.11.** Possuir um Dashboard com as principais informações referentes ao ambiente;
- 4.3.2.12.** Ter a capacidade de visualizar em modo gráfico, através de mapas, os fluxos de dados do ambiente;
- 4.3.2.13.** Ser possível visualizar de forma agregada o fluxo de dados, de forma gráfica, de um período de tempo, como 30 dias por exemplo;
- 4.3.2.14.** Visualizar todos os ativos protegidos, incluindo informações como Nome, Sistema Operacional, Número de CPUs e IP;
- 4.3.2.15.** Ter a capacidade de visualizar todas as etiquetas associadas a um único dispositivo;
- 4.3.2.16.** Ser possível criar novas etiquetas e gerenciar etiquetas existentes;
- 4.3.2.17.** Exportar as etiquetas, no mínimo em CSV ou XLS;
- 4.3.2.18.** Ter a capacidade, através de interface gráfica na própria console, de monitorar a saúde de todos os componentes da solução;
- 4.3.2.19.** Ter a capacidade de atualizar os agentes instalados nos ativos de forma centralizada pela própria console, sem necessitar de execução manual no ativo ou de uso de scripts;
- 4.3.2.20.** Deve possuir Logs de Auditoria, para no mínimo: autenticação, políticas de segmentação, etiquetas, consulta de logs.
- 4.3.2.21.** Os Logs de Auditoria devem conter, no mínimo: O dia, hora, Evento, Nome do usuário, IP de Origem e Descrição;



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- 4.3.2.22.** Deve ser possível gerenciar os usuários com acesso a solução, não havendo limites para o número de usuários existentes;
- 4.3.2.23.** Deve suportar autenticação Kerberos;
- 4.3.2.24.** Deve ser possível criar usuários locais, e gerenciar os usuários existentes.
- 4.3.2.25.** Deve suportar segundo fator de autenticação;
- 4.3.2.26.** Possuir níveis de permissões diferentes para os usuários, no mínimo: Administrador, Somente Leitura, Visualização de Incidentes, Administração de Políticas.
- 4.3.2.27.** Deve possuir mecanismo de busca dos incidentes;
- 4.3.2.28.** Deve ser possível customizar o nível de criticidade dos incidentes;
- 4.3.2.29.** Deve ser possível trabalhar com múltiplos sites, em console única e que permitam aos usuários aplicar seletivamente políticas e regras a um conjunto de ativos nessa localização;
- 4.3.2.30.** Deve ser possível gerenciar a administração de políticas em vários sites/divisões gerenciando os escopos dos usuários por site;
- 4.3.2.31.** Deve ser possível ao administrador total autonomia para criar, modificar e excluir regras, além de visualizar todos os logs para Ativos atribuídos aos seus sites;

4.3.3. Agentes de Microsegmentação

- 4.3.3.1.** A solução deve disponibilizar agentes instaláveis nos ativos protegidos, compatíveis com sistemas operacionais Windows e Linux, ambientes virtualizados (VMware, Hyper-V) e contêineres (Docker, Kubernetes, OpenShift). O licenciamento deverá ser baseado em agente por nó do cluster, sendo cada nó de trabalho (worker node) considerado uma unidade de licenciamento.
 - Todos os contêineres/pods que executarem nos nós licenciados deverão estar cobertos pelo licenciamento, independentemente da quantidade de contêineres em cada nó;
 - Não será exigido licenciamento individual por contêiner ou pod, considerando-se apenas a instalação e operação do agente no nó;



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- A administração de políticas, microssegmentação e monitoramento deverá se estender a todos os workloads presentes nos nós licenciados.
- 4.3.3.2.** A instalação dos agentes deve suportar métodos manuais e automatizados, incluindo MSI, scripts PowerShell, Ansible ou equivalente.
- 4.3.3.3.** Deve possibilitar a instalação do agente de forma manual, através de MSI e scripts já elaborados.
- 4.3.3.4.** Os agentes devem operar inicialmente em modo de monitoramento, fornecendo visibilidade detalhada do tráfego, podendo posteriormente aplicar políticas de segurança de forma controlada.
- 4.3.3.5.** Os agentes devem consumir não mais que 5% de recursos de CPU e Memória RAM;
- 4.3.3.6.** Os agentes deverão alimentar continuamente a console central.
- 4.3.3.7.** Atualizações e manutenção dos agentes devem poder ser realizadas sem interrupção das operações críticas do ativo protegido.
- 4.3.3.8.** Deverá suportar a instalação de agentes em diversos sistemas operacionais listados (Amazon Linux, CentOS, Oracle Linux, Redhat, Debian, Ubuntu, Windows, MacOS, etc.).
- 4.3.3.9.** No caso de dispositivos que não possam receber os agentes, a solução deve disponibilizar um mecanismo que permita cadastrar os mesmos e criar regras para ditar como estes recursos podem interagir com a rede protegida.
- 4.3.3.10.** Deve suportar a instalação dos agentes em nuvens públicas ou privadas, independente do provedor.
- 4.3.3.11.** Deverá ser independente de hardware.
- 4.3.3.12.** O processo de remoção e atualização dos agentes deverá seguir os mesmos modelos já definidos de instalação.
- 4.3.3.13.** A comunicação entre o agente e a console central deve ser criptografada.
- 4.3.3.14.** O agente deve ser compatível com, pelo menos, as seguintes versões de Sistema Operacionais:



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- CentOS Stream release 9
- Microsoft Windows 11 (64-bit)
- Microsoft Windows 10 (64-bit)
- Microsoft Windows 7 (32-bit)
- Microsoft Windows Server 2003 (64-bit)
- Microsoft Windows Server 2003 Standard (32-bit)
- Microsoft Windows Server 2016 (64-bit)
- Microsoft Windows Server 2022 (64-bit)
- OpenShift 4.18
- Oracle Linux 7 (64-bit)
- Red Hat Enterprise Linux CoreOS release 4.18
- SUSE Linux Enterprise 10 (32-bit/64-bit)
- SUSE Linux Enterprise 11 (64-bit)
- SUSE Linux Enterprise 12 (64-bit)
- SUSE Linux Enterprise 15 (64-bit)
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Linux 22.04 e superiores (64-bit)

4.3.4. Visibilidade do Tráfego

- 4.3.4.1.** A solução deve fornecer visibilidade detalhada de todo o tráfego entre ativos (leste-oeste e norte-sul).
- 4.3.4.2.** Devem ser fornecidos dashboards atualizados em tempo real.
- 4.3.4.3.** A solução deve gerar alertas configuráveis para eventos suspeitos, nativamente ou por meio de customização por API ou integrações.
- 4.3.4.4.** Todo o histórico de eventos deve ser armazenado de forma segura.
- 4.3.4.5.** A solução deverá fornecer um mapa de dependência de aplicativos em tempo real.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- 4.3.4.6.** A solução deverá fornecer meios para filtragem específica de comunicações em log na console.
- 4.3.4.7.** A visão detalhada do tráfego de rede deverá mostrar os processos responsáveis por cada comunicação.
- 4.3.4.8.** A visibilidade deverá suportar conceitos de RBAC.
- 4.3.4.9.** Os dados de visibilidade deverão estar disponíveis por pelo menos 90 dias.
- 4.3.4.10.** Deve possibilitar filtragem de tráfego com base em aplicações, rótulos, ambientes, etc.
- 4.3.4.11.** Não deve haver limitação de número de regras ou tráfego analisado.
- 4.3.4.12.** Criação e Aplicação de Regras
- 4.3.4.13.** A solução deve permitir definição de regras baseadas em contexto (usuário, grupo, aplicação, processo ou atributos de rede).
- 4.3.4.14.** As regras deverão permitir, no mínimo, o uso dos seguintes atributos de rede: Listas de IPs, sub-redes, FQDNs, range de portas e portas customizadas.
- 4.3.4.15.** Deve suportar portas dinâmicas baseadas em processo do SO.
- 4.3.4.16.** A solução deverá permitir criação de rótulos aplicados às cargas de trabalho.
- 4.3.4.17.** Os rótulos deverão suportar conceito de escopo da rede.
- 4.3.4.18.** Rótulos e atributos de contexto devem estar disponíveis para criação de políticas.
- 4.3.4.19.** Regras deverão possibilitar criação granular baseado em rótulos e atributos de contexto.
- 4.3.4.20.** As regras devem possibilitar controle granular de fluxos e registro completo de auditoria.
- 4.3.4.21.** A solução deve realizar sugestões inteligentes de como a regra deverá ser criada.
- 4.3.4.22.** A visão detalhada dos logs deve permitir a criação de regras a partir de logs.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- 4.3.4.23.** Deve ser possível simular a aplicação das regras antes de ativá-las.
- 4.3.4.24.** A aplicação das políticas deve ser automática e dinâmica.
- 4.3.4.25.** Deve permitir duplicação de políticas pelo administrador.
- 4.3.4.26.** A solução deverá possuir templates de política para serviços corporativos (AD, SQL, Exchange, WSUS, etc.).
- 4.3.4.27.** A solução deverá permitir atribuição de políticas em grupos ou hosts específicos.
- 4.3.4.28.** No caso de remoção do agente, todas as regras criadas deverão ser removidas.
- 4.3.4.29.** A solução deverá possuir integração nativa com scanners de vulnerabilidade. Integração deverá suportar Qualys, Tenable ou Rapid7.
- 4.3.4.30.** A solução deverá permitir integração com LDAP, LDAPS e Active Directory para controle baseado em grupos.
- 4.3.4.31.** A solução deverá suportar visualização de impacto das políticas antes da aplicação de modificações.
- 4.3.4.32.** A visibilidade deverá permitir identificar tráfegos associados a políticas específicas.
- 4.3.4.33.** A solução deverá suportar controle de políticas inbound e outbound.
- 4.3.4.34.** Deve ser possível criação de regras para isolamento de ativos na rede.
- 4.3.4.35.** Políticas devem possibilitar coexistência com políticas de firewall existentes.
- 4.3.4.36.** Deve permitir identificação e proteção de ativos sem agente.

4.3.5. API e Integrações

- 4.3.5.1.** A solução deve possuir uma API forte e bem documentada.
- 4.3.5.2.** Via API deve ser possível realizar operações em políticas e controlar os ativos da solução.
- 4.3.5.3.** Deve ser baseada em HTTPS e ser compatível com métodos GET, PUT, POST e DELETE.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- 4.3.5.4.** Deve ser autenticada via chave a ser gerada no portal da solução.
- 4.3.5.5.** Deve possibilitar integração com ferramentas DevOps como Chef, Puppet ou Ansible.
- 4.3.5.6.** Deve possuir integração com SIEMs como QRadar, Splunk ou ArcSight.
- 4.3.5.7.** Logs exportáveis em formatos JSON, CEF, LEEF.

4.4. Requisitos de Serviços

4.4.1. Especificações Gerais dos Serviços

- 4.4.1.1.** Os serviços que eventualmente acarretem risco para os sistemas em produção da ALESP, ou que requeiram parada de serviços em execução, somente poderão ser executados fora de expediente, em horários previamente acordados com a área de TI da ALESP.
- 4.4.1.2.** A CONTRATADA designará profissional indicado como Gerente de Projeto, como sendo o ponto único de contato da ALESP, para acompanhamento das atividades previstas no Cronograma apresentado no Plano de Implantação, bem como apresentará processo de escalonamento de problemas durante e após a implantação da solução.
 - O Gerente de Projeto deverá possuir a certificação PMP – Project Management Professional do PMI – Project Management Institute.
 - O Gerente de Projeto será o responsável pelo gerenciamento dos prazos, resultados e qualidade da implementação da solução por parte da CONTRATADA, controlando todos os SLAs e os respectivos entregáveis de cada etapa definidos neste documento, que deverão contar no Cronograma do Plano de Implantação;
- 4.4.1.3.** A CONTRATADA deverá indicar, no mínimo, 01 (um) Especialista Técnico, funcionário ou contratado da empresa, que será o responsável pela implementação das tecnologias e soluções contratadas.
 - O Especialista Técnico deverá possuir certificação oficial do fabricante e experiência comprovada em implantação, configuração e administração da solução em ambientes corporativos.
 - O Especialista Técnico será responsável pela implantação (i.e., instalação, ativação, configuração/customização), operação



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

assistida e resolução de questões técnicas da solução, visando garantir a correta implantação e funcionamento do objeto.

4.4.1.4. A CONTRATADA deverá disponibilizar, durante todas as fases do projeto, um “Technical Account Manager (TAM)” ou “Technical Adoption Manager”, profissional que seja funcionário ou representante oficial do fabricante da solução, com certificação ou experiência comprovada, para acompanhamento técnico das atividades de planejamento, implantação, operação assistida e suporte/manutenção da solução.

- O TAM terá as seguintes atribuições mínimas:

4.4.1.4..1. Atuar como ponto de contato técnico direto entre a CONTRATANTE e o fabricante da solução.

4.4.1.4..2. Auxiliar no planejamento e validação do Plano de Implantação.

4.4.1.4..3. Orientar a equipe da CONTRATANTE durante a instalação, configuração, testes e aceitação da solução.

4.4.1.4..4. Fornecer suporte técnico especializado em dúvidas e incidentes durante a operação assistida e manutenção.

4.4.1.4..5. Garantir transferência de conhecimento sobre melhores práticas de operação, administração e atualização da solução.

- O TAM não precisa ser dedicado exclusivamente à CONTRATANTE, podendo ser compartilhado com outros clientes, desde que a disponibilidade mínima necessária para acompanhamento do projeto e atendimento dos marcos de implantação, operação assistida e suporte seja garantida.

4.4.1.5. Todos os profissionais elencados acima deverão ser formalmente designados pela CONTRATADA e descritos no Plano de Implantação aceito. A CONTRATADA terá até 5 dias corridos, contados a partir da assinatura do contrato, para designar formalmente os profissionais de sua equipe (i.e., Gerente de Projetos e Especialista(s) Técnico da Solução) que participarão do projeto. Neste prazo, os profissionais mencionados deverão ser apresentados à equipe técnica da ALESP para reunião inicial de alinhamento.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

4.4.1.6. A ALESP, a qualquer momento e a seu exclusivo critério, durante as fases Capacitação Técnica, de elaboração do Plano de Implantação, Implantação/Ativação da Solução, Horas de projeto sob demanda, Operação Assistida, Suporte Técnico e Manutenção, poderá solicitar à CONTRATADA a substituição de qualquer profissional, membro de sua equipe técnica, que esteja prestando serviços para a ALESP. Por isso, a CONTRATADA deverá substituir o referido membro de equipe, indicando um substituto, igualmente certificado e qualificado, em até 5 dias corridos após a comunicação da ALESP. Neste caso, a ALESP terá até 5 dias corridos para nova análise da Equipe da CONTRATADA, não interrompendo a contabilização de prazo da respectiva fase em andamento.

4.4.2. Plano de Implantação (ITEM 1)

4.4.2.1. A CONTRATADA deverá elaborar e entregar à ALESP um documento chamado Plano de Implantação, que contemple todos os requisitos especificados neste memorial, bem como todas as funcionalidades necessárias para o correto funcionamento da solução adquirida. O principal objetivo do Plano de Implantação da CONTRATADA será auxiliar a ALESP a mitigar potenciais riscos da implementação das tecnologias e soluções contratadas, avaliando os Planos de Ação sugeridos para cada risco identificado/previsto, deliberando sobre tais ações.

4.4.2.2. Escopo e Objetivo

- O Plano de Implantação deve detalhar todas as atividades necessárias para a instalação, configuração e ativação da solução de microsegmentação em ambientes corporativos heterogêneos da CONTRATANTE, incluindo servidores físicos, virtualizados e containerizados.
- Deve garantir a entrega de uma solução pronta para operação conforme especificações do TR, incluindo SaaS dedicado ou On-Premises.

4.4.2.3. O Plano de Implantação deverá ser entregue em mídia eletrônica (PDF, DOCX, XLSX ou PPTX), contemplando, no mínimo, as seguintes etapas:

- **Planejamento e Preparação**



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

4.4.2.3..1. Mapeamento do ambiente atual: servidores físicos, VMs, contêineres, redes e VLANs.

4.4.2.3..2. Identificação de requisitos de compatibilidade (VMware vSphere 7.0.3+, contêineres Kubernetes/OpenShift/Docker, nuvens públicas, Active Directory, LDAP, F5).

4.4.2.3..3. Definição de agentes a serem instalados por nó ou dispositivo.

4.4.2.3..4. Cronograma: detalhamento das fases, atividades, dependências, responsáveis, marcos de aceite e datas de início e término.

4.4.2.3..5. Plano de Comunicação: periodicidade de reuniões, relatórios e responsáveis.

4.4.2.3..6. Equipe e Organograma dos profissionais envolvidos.

4.4.2.3..7. Matriz de Responsabilidades (RACI).

4.4.2.3..8. Plano de Ação e Mitigação de Falhas identificadas.

4.4.2.3..9. Lista de recursos de hardware e software a serem utilizados.

- **Instalação e Configuração**

4.4.2.3..1. Instalação da solução em modo SaaS dedicado ou On-Premises.

4.4.2.3..2. Implantação dos agentes nos ativos protegidos (Windows, Linux, contêineres) manual ou automatizada (MSI, PowerShell, Ansible).

4.4.2.3..3. Configuração de alta disponibilidade, redundância e sincronização entre instâncias.

4.4.2.3..4. Implementação de controle de acesso baseado em funções (RBAC) e autenticação via SAML/OAuth/Kerberos, incluindo integração com IdPs existentes (ex.: Micro Focus NAM, Azure AD).

- **Mapeamento e Etiquetamento**

4.4.2.3..1. Descoberta e etiquetamento de todos os ativos (com ou sem agente).



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

4.4.2.3..2. Criação de grupos de ativos e políticas iniciais de microsegmentação.

4.4.2.3..3. Configuração de ilhas de isolamento e controle de comunicação entre ativos.

- **Definição de Políticas de Segurança**

4.4.2.3..1. Criação de políticas baseadas em contexto (usuário, grupo, aplicação, processo, atributos de rede).

4.4.2.3..2. Teste e simulação das políticas antes da aplicação efetiva.

4.4.2.3..3. Aplicação automatizada de políticas e integração com firewalls existentes.

- **Treinamento e Transferência de Conhecimento**

4.4.2.3..1. Treinamento para administradores e usuários da CONTRATANTE.

4.4.2.3..2. Documentação detalhada do ambiente, políticas, procedimentos de atualização e recuperação de desastres.

- **Testes e Validação**

4.4.2.3..1. Teste de alta disponibilidade, failover e continuidade de serviço.

4.4.2.3..2. Teste de aplicação de políticas em ambientes de produção simulada.

4.4.2.3..3. Validação da visibilidade do tráfego (leste-oeste e norte-sul) e relatórios de auditoria.

- Outras informações que possam ser requeridas pela CONTRATANTE.

4.4.3. Implantação da Solução (ITEM 3)

4.4.3.1. Escopo do Serviço

- O serviço inclui todas as atividades necessárias para instalar, configurar, parametrizar e ativar a solução de microsegmentação em ambientes físicos, virtualizados e containerizados da CONTRATANTE.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- Deve contemplar integração com sistemas existentes, validação de políticas, testes de funcionamento e entrega de documentação e treinamento.
- Os componentes da solução deverão ser instalados em sua última versão validada pelo fabricante, somente sendo admitida a utilização de uma versão inferior em comum acordo com a ALESP.

4.4.3.2. Fazem parte da instalação e são responsabilidades da CONTRATADA:

- **Configuração de infraestrutura** - Preparação dos servidores, redes e VLANs segundo melhores práticas de segurança e compatibilidade com a solução.
- **Instalação da solução** - Instalação de console, agentes e componentes SaaS/On-Premises, incluindo alta disponibilidade e redundância.
- **Etiquetamento de ativos** - Identificação e etiquetamento de todos os ativos (com ou sem agente), definição de grupos e ilhas de isolamento.
- **Configuração de políticas** - Criação de regras de microsegmentação, controle de tráfego, isolamento e políticas contextuais (usuário, grupo, aplicação).
- **Integração com sistemas existentes** - Integração com IdP (SAML/OAuth) e outras integrações que, eventualmente, sejam identificadas no planejamento.
- **Testes e validação** - Validação de alta disponibilidade, failover, aplicação de políticas, visibilidade do tráfego e auditoria.
- **Repasse de conhecimento e documentação** - Capacitação da equipe da CONTRATANTE e entrega de documentação detalhada do ambiente, políticas e procedimentos.
- **Plano de continuidade** - Procedimentos de reversão, backup, recuperação e atualização de agentes sem interrupção

4.4.3.3. Outros requisitos do serviço de implantação



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- Todos os serviços devem ser prestados por especialistas certificados e com experiência comprovada em microsegmentação.
 - Os agentes instalados devem operar em modo monitoramento inicialmente e aplicar políticas de forma controlada, sem impactar operações críticas.
 - A comunicação entre agentes e console deve ser 100% criptografada.
 - O serviço deve garantir alta disponibilidade, redundância e sincronização em tempo real.
 - Deverá ser providenciada integração completa com a infraestrutura existente, incluindo firewalls, sistemas de identidade e soluções de monitoramento.
 - O serviço inclui reparo imediato de quaisquer danos causados à infraestrutura da CONTRATANTE durante a implantação.
 - Caso o fabricante publique o anúncio de *End of Life* da solução antes do aceite da implantação, o fornecedor deve substituir o modelo por equivalente ou superior à solução que entrou em fim de linha.
- 4.4.3.4.** A CONTRATADA deverá fornecer, ao final da implantação, a documentação de como a solução foi implementada "*As Built*", contendo, no mínimo:
- Versão exata de cada componente instalado (console, agentes, módulos SaaS/On-Premises).
 - Configurações aplicadas: políticas de microsegmentação, regras de firewall, etiquetas, grupos de usuários, ilhas de isolamento.
 - Parâmetros de integração: IdPs, LDAP, Active Directory, SIEM, scanners de vulnerabilidade, APIs, outros.
 - Topologia final: diagrama de rede, VLANs, servidores, clusters, contêineres.
 - Ambiente de testes: resultados de testes de funcionalidade, failover, alta disponibilidade e visibilidade de tráfego.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- Procedimentos executados: scripts, métodos de instalação automatizados/manuais, etapas de aplicação de políticas.

4.4.3.5. A documentação de “*As Built*” deverá ser entregue em formato PDF, DOCX, XLSX ou PPTX e submetida à validação e aceite da CONTRATANTE.

4.4.4. Operação Assistida (ITEM 4)

4.4.4.1. Após a implantação e devido aceite da solução, será dado início à fase de Operação Assistida, que inclui acompanhamento técnico com monitoramento do ambiente implantado, supervisão prática das rotinas, implementação de ajustes e entrega de procedimentos à equipe da Contratante, garantindo autonomia, qualidade e continuidade das operações.

4.4.4.2. Durante a Operação Assistida, a solução implantada é acompanhada e monitorada continuamente pelo especialista técnico que realizou a implantação para garantir seu correto funcionamento, estabilidade e desempenho. Essa fase inclui supervisão prática das rotinas de operação e manutenção, execução de ajustes e melhorias necessárias, bem como validação da qualidade e confiabilidade do ambiente, assegurando a continuidade das operações.

4.4.4.3. O serviço de Operação Assistida objetiva:

- Garantir de que os produtos sejam operados dentro das melhores práticas recomendadas.
- Elevar o desempenho e a disponibilidade do produto no início da sua operação, assegurado pela capacitação prática dos operadores em condições reais, suportados *on site* por especialistas capazes de assegurar que todos os procedimentos sejam realizados de acordo com os padrões recomendados.
- Consolidar a autonomia da equipe interna, corrigir eventuais falhas remanescentes, implementar melhorias identificadas e assegurar a qualidade e a continuidade das operações.

4.4.4.4. Durante a Operação Assistida deverá ser prestado todo o suporte necessário para a operacionalidade dos produtos, minimizando o risco na implantação de novas tecnologias e proporcionando as condições ideais para transferência da tecnologia envolvida em regime *on the job training*, para que a ALESP possa assumir as atividades com sua própria equipe.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

4.4.4.5. Durante este período, o corpo técnico especialista que realizou a implantação deverá permanecer à disposição da ALESP, de modo a oferecer suporte na realização de testes, análises, medidas e ajustes, assegurando que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos.

4.4.4.6. O serviço de Operação Assistida inclui as seguintes atividades:

- Execução de atividades operacionais, utilizando os procedimentos recomendados a cada rotina.
- Análise de métricas, logs e indicadores de disponibilidade, performance e confiabilidade.
- Aplicação de atualizações e patches, realização de testes de contingência e simulações de falhas para validar resiliência.
- Registro detalhado das atividades realizadas, incidentes resolvidos e fornecimento de relatórios periódicos com ajustes e recomendações.
- Apoio na integração de novos processos ou ferramentas, supervisão de procedimentos críticos e preparação da equipe da Contratante para assumir integralmente a operação.
- Execução de atividades de manutenção corretiva, utilizando os procedimentos que permitam maior eficiência e eficácia na solução de falhas.
- Execução de atividades de manutenção preventiva, rotinas de testes, análises e medidas, utilizando os procedimentos que assegurem mínima interferência na operação e máxima disponibilidade dos produtos.
- Elaboração de procedimentos especiais ou detalhamento dos procedimentos padrão, caso seja necessário;
- Registro detalhado das atividades realizadas, incidentes resolvidos e fornecimento de relatórios periódicos com ajustes e recomendações;

4.4.4.7. Ao final da Operação Assistida, a CONTRATADA deverá entregar à ALESP:



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- Procedimentos customizados de O&M (Operação e Manutenção), possibilitando que o cliente assuma as atividades com sua própria equipe no menor tempo possível.
- Relatório ao final do período de operação contendo informações sobre atividades executadas e recomendações sobre como executar as atividades de O&M com efetividade e eficácia.

4.4.5. Serviço continuado de suporte e manutenção pelo período de 21 meses. (ITEM 6)

- 4.4.5.1.** A CONTRATADA deverá atender as condições de SLA previstas no item 7.2.2 e se sujeitar às definições de descontos do item 7.2.3 em caso de descumprimento dos níveis de serviço.
- 4.4.5.2.** A CONTRATADA deverá prover a evolução do produto, disponibilizando qualquer atualização, melhoria ou correção introduzida nos produtos que componham a solução.
- 4.4.5.3.** A CONTRATADA deverá prover a manutenção da solução, assim entendida a correção de erros de funcionamento ou desempenho inconsistente com as especificações técnicas dos produtos.
- 4.4.5.4.** CONTRATADA deverá atuar na resolução de problemas de atualização da solução, upgrade, salvamento e restauração.
- 4.4.5.5.** A CONTRATADA deverá fornecer qualquer informação relativa ao funcionamento da solução, dirimindo as dúvidas ou problemas operacionais na sua utilização.
- 4.4.5.6.** A CONTRATADA deverá prover acesso ao ambiente de disseminação de conhecimento e atualização da solução, de preferência via internet, à equipe técnica da ALESP.
- 4.4.5.7.** A CONTRATADA deverá acompanhar os testes e a homologação, caso a ALESP julgue necessário, dos novos produtos ou pacotes de atualização disponibilizados pelo fabricante.
- 4.4.5.8.** A prestação dos serviços de suporte técnico deverá ser realizada por profissional devidamente certificado para atender às necessidades da ALESP em todos os aspectos da solução, com as atribuições descritas a seguir:



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- Fornecer orientação, recomendações de melhores práticas, produzir materiais e promover a divulgação interna da solução através de workshops ou outros métodos acordados com a ALESP.
 - Promover a transferência de conhecimento através de esclarecimento de dúvidas sobre a configuração e operacionalização dos produtos.
 - Desenvolver automações e integrações para reduzir o custo operacional e risco de falhas no uso da solução.
 - Executar a extração de dados e montagem de relatórios relacionados à solução, quando solicitado.
 - Identificar, defender e executar a atualização de componentes ou patches recomendados pelo fabricante.
 - Apresentar relatórios de chamados e suporte técnico com informações e formato solicitado pela ALESP.
 - Tratar incidentes relacionados ao funcionamento e configuração da solução, buscando identificar a causa raiz através de troubleshooting.
 - Criar, alterar, excluir e consultar registros na solução de acordo com requisições de serviços abertas pela ALESP.
 - Conduzir a abertura e acompanhamento de chamados junto ao fabricante, de forma a respeitar todos os prazos de Níveis Mínimos de Serviço Exigidos (NMSE) definidos.
 - Auxiliar o time técnico da ALESP na ativação/migração dos serviços para a nova solução.
- 4.4.5.9.** O profissional em suporte técnico deverá cumprir todos os padrões de segurança e regras de controle de acesso determinados pela ALESP.
- 4.4.5.10.** Os serviços do suporte deverão estar disponíveis 24 (vinte e quatro) horas por dia 7 (sete) dias por semana.
- 4.4.5.11.** Os serviços de suporte técnico, quando em trabalho local, serão prestados no endereço abaixo, ou em outra dependência da ALESP, por este indicada, localizada à Av. Pedro Álvares Cabral, 201 São Paulo · CEP 04097-900 (SP).



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

4.4.5.12. Se, em caráter de exceção, houver necessidade de que os serviços do suporte local sejam executados nos finais de semana e feriados, ou em um período maior que 8 (oito) horas diárias, ou que sejam realizados no período após as 22h, a ALESP deverá negociar previamente esta necessidade com a CONTRATADA.

4.4.5.13. A CONTRATADA terá total responsabilidade pelo controle de frequência, disciplina e pelo cumprimento de todas as obrigações trabalhistas, fiscais e previdenciárias, inclusive decorrentes de acidentes, indenizações, multas, seguros, pagamentos a fornecedores diretos, normas de saúde pública e regulamentadoras do trabalho, assim como pelo cumprimento de todas as demais obrigações atinentes à prestação dos serviços.

4.4.5.14. Todo procedimento ou parametrização, inclusive suas documentações, desenvolvida pelo suporte dedicado no ambiente da ALESP, utilizando os meios disponibilizados pela SOLUÇÃO, será de propriedade exclusiva da ALESP, excluídas as documentações oficiais do fabricante de produtos da CONTRATADA.

4.4.6. Treinamento Oficial (ITEM 5)

4.4.6.1. A Contratada deverá fornecer treinamento técnico oficial, ministrado ou credenciado pelo fabricante da solução, antes da entrega do plano de implantação, para até 6 profissionais indicados pela Contratante.

4.4.6.2. O treinamento deverá abranger, no mínimo:

- Arquitetura, topologia e componentes da solução de microssegmentação.
- Modelagem e definição de políticas de segmentação granular.
- Requisitos técnicos, integrações com infraestrutura de rede e sistemas de segurança existentes.
- Procedimentos detalhados de instalação, configuração e implantação das regras de microssegmentação.
- Políticas de segurança, perfis de acesso, controle de fluxo e isolamento de segmentos.
- Monitoramento, auditoria e resposta a incidentes específicos da microssegmentação.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- Ferramentas de gestão e visualização de segmentação, análise de logs e geração de relatórios.
- Procedimentos para atualização, manutenção e troubleshooting da solução.

4.4.6.3. A carga horária mínima será de 40 horas/aula, devendo ser fornecido material didático oficial e certificado emitido pelo fabricante ou representante autorizado, com menção expressa à carga horária realizada.

4.4.6.4. Realização obrigatória de laboratórios práticos, com exercícios que contemplem cenários reais de integração, configuração, testes de regras de microssegmentação, simulação de incidentes e aplicação de políticas de segurança, garantindo a comprovação da aprendizagem dos participantes.

4.4.6.5. O curso deverá compor a trilha oficial de certificação do fabricante para carreiras técnicas, não sendo aceito treinamento da área comercial ou cursos introdutórios superficiais.

4.4.7. Horas de Projeto Sob Demanda (ITEM 7)

4.4.7.1. Fica incluído nesta contratação um banco de horas de serviços técnicos especializados, destinado a ajustes, expansões ou reconfigurações da solução contratada, a ser disponibilizado junto com o período de “Serviço continuado de Suporte e manutenção”, após conclusão da “Operação assistida”.

4.4.7.2. O banco de horas será de 300 horas ao longo da vigência contratual, com possibilidade de uso fracionado, observado o mínimo de 4 (quatro) horas por ordem de serviço.

4.4.7.3. Os serviços deverão ser prestados exclusivamente por profissionais com o mesmo perfil, certificações e qualificações exigidos para a implantação inicial.

4.4.7.4. O prazo de início de atendimento será de no máximo 5 dias úteis a partir da solicitação formal.

4.4.7.5. As horas sob demanda poderão ser utilizadas exclusivamente para:

- Implementação de novas funcionalidades ou recursos oficialmente previstos pelo fabricante da solução.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- Ajustes e reconfigurações em parâmetros, regras e políticas da solução que sejam necessários em decorrência de mudanças no ambiente tecnológico da Contratante e que demandem planejamento detalhado, análise de impacto e validação formal prévia.
- Integração da solução com novos sistemas, plataformas ou serviços complementares.
- Expansão, atualização ou customização de módulos e componentes contemplados no escopo da solução contratada.

4.4.7.6. Toda e qualquer alteração realizada no âmbito das horas sob demanda deverá ser documentada, seguindo o mesmo formato e padrão técnico da documentação de implantação inicial, sendo obrigatória a atualização da documentação principal do projeto “*As Built*” e a entrega de nova versão consolidada à Contratante.

4.4.7.7. O uso das horas de projeto sob demanda deverá ser previamente aprovado pela Contratante e registrado em ordem de serviço, abatendo-se do saldo total contratado.



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

5. ALTERNATIVAS POSSÍVEIS

Id	Descrição da solução (ou cenário)
1	Segmentação tradicional com VLANs e ACLs Utiliza o modelo atual com separação lógica por VLANs e regras ACL nos switches e roteadores. É uma abordagem amplamente conhecida e de baixo custo direto, mas com limitações importantes em granularidade, visibilidade de tráfego interno e resposta a ameaças. Requer gestão manual intensiva, tem baixa automação, dificuldade de escalar em ambientes complexos e é suscetível a erros operacionais. Indicado para estruturas estáticas e pouco sujeitas a mudanças ou riscos elevados. Exemplos de fornecedores incluem Cisco, HPE Aruba e Juniper Networks.
2	Firewall interno distribuído Aplica regras de filtragem e controle de tráfego entre workloads usando recursos de firewall. Fornece mais controle que o modelo tradicional, com possibilidade de segmentação em camadas mais finas da rede. Entretanto, a dependência de políticas estáticas e a necessidade de gestão centralizada podem aumentar a complexidade. A escalabilidade e integração com identidades também podem ser limitadas. Exemplos de fornecedores incluem Fortinet, Palo Alto Networks e Check Point.
3	Microsegmentação baseada em identidade e contexto Proporciona segmentação lógica com base em identidades de usuários, aplicações e contexto operacional (como localização, função, comportamento e risco). Permite políticas dinâmicas, aplicação adaptativa de controles, visibilidade em tempo real do tráfego e resposta automatizada a incidentes. Pode ser integrada a fontes de identidade (como AD) e oferece alto grau de automação e escalabilidade. Exige implantação planejada e integração com ferramentas existentes. Indicado para ambientes complexos, com foco em proteção lateral e adesão a princípios de Zero Trust. Exemplos de fornecedores incluem Illumio, Akamai e Cisco.



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

Análise Comparativa das Soluções			
Requisitos	Cenários		
	Cenário 1	Cenário 2	Cenário 3
Suporte e Manutenção	Atende	Atende	Atende
Segmentação de ambientes	Atende	Atende	Atende
Isolamento de workloads e serviços críticos	Atende	Atende	Atende
Geração de logs completos de comunicação leste-oeste para auditoria.	Não atende	Não atende	Atende
Controle granular baseado em identidade, função e contexto de risco.	Não atende	Não atende	Atende
Mapeamento em tempo real de fluxos e sistemas conectados	Não atende	Não atende	Atende
Controle granular baseado em identidade, função e contexto de risco.	Não atende	Não atende	Atende
Controle de dispositivos em conformidade para acesso à rede.	Não atende	Não atende	Atende
Correlação usuário, dispositivo e IP	Não atende	Não atende	Atende
Visibilidade dos ativos da rede em tempo real	Não atende	Não atende	Atende
Automação de resposta a incidentes	Não atende	Não atende	Atende
Resultado da Análise	Não viável	Não viável	Viável



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

Realizou-se também pesquisa sobre contratações análogas deste objeto realizadas por entidades públicas através do Portal Nacional de Contratações Públicas (<https://www.gov.br/pncp/pt-br>) e obteve-se os seguintes resultados:

Edital nº 201/2025

Id contratação PNCP: 16636540000104-1-000027/2025

Fonte: Portal de Compras do Estado de Minas Gerais

Órgão: CIA DE TECNOLOGIA DA INFORMACAO DO ESTADO DE MG

Unidade compradora: 5141001 - GERENCIA DE COMPRAS

Objeto: O objeto da presente licitação é o registro de preços para eventual e futura contratação de licenciamento de agentes de Solução de Microsegmentação Guardicore, incluindo atualização de versões e suporte técnico, conforme condições, quantidades e exigências estabelecidas neste Edital e seus Anexos.

Preço Total Homologado da Compra: R\$ 8.108.000,00

Licitante: SHIELD SECURITY TECNOLOGIA LTDA - CNPJ: 31.746.312/0001-72

Qtd: 1.000 licença por servidor

Prazo: 24 meses

Edital nº 01/2025/2025

Id contratação PNCP: 13937032000160-1-000044/2025

Fonte: Licitações-E BB

Órgão: ESTADO DA BAHIA

Unidade compradora: 000000055 - PRODEB - CIA DE PROCESSAMENTO DE DADOS DA BAHIA

Objeto da licitação: Implantação de sistema de registro de preços objetivando a formalização de ata com o vencedor do certame, visando a contratação de solução de cibersegurança com microssegmentação, visibilidade e proteção de rede, para os servidores e containers hospedados no Data Center da Prodeb, na modalidade de subscrição de licença, incluindo suporte técnico no regime 24x7 (vinte e quatro horas por dia, sete dias por semana) e garantia de atualização das versões pelo período de 36 meses, contemplando também, instalação, configuração e treinamento, de acordo com



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

as especificações técnicas mínimas e detalhamentos consignados neste Termo de Referência (TR) e seus anexos.

Valor total estimado: R\$ 9.590.306,00

Nome ou razão social do fornecedor: COMDADOS COMERCIO E SERVICOS ELETRONICOS LTDA

Qtd e valores estimados:

Item 1: 500 Licença por servidor

- R\$ 387,87 (Un/mensal) | R\$ 13.963,32 (Un/36meses) | R\$ 6.981.660,00 (Total)

Item 2: 50 Licenças por nós de containers

- R\$ 1.224,82 (Un/mensal) | R\$ 44.093,52 (Un/36meses) | R\$ 2.204,676,00 (Total)

Item 3: Treinamento 4 participantes

- R\$ 19.635,00 (Un) | R\$ 78.540,00 (Total)

Item 4: Instalação e configuração item 1

- R\$ 488,88 (Un) | R\$ 244.000,00 (Total)

Item 5: Instalação e configuração item 2

- R\$ 1.628,60 (Un) | R\$ 81.430,00 (Total)

Prazo: 36 meses

Edital nº 17/2024fer/2024

Id contratação PNCP: 76276849000154-1-000070/2024

Fonte: Licitações-E BB

Órgão: MINISTERIO PUBLICO DO ESTADO DE SANTA CATARINA PROCURADORIA GERAL DE JUSTICA

Unidade compradora: 000000001 - MINISTERIO PUBLICO ESTADO SANTA CATARINA

Objeto: Aquisição de licenças e serviços para solução tecnológica de cibersegurança para microssegmentação de cargas de trabalho (workloads) Akamai Guardicore, conforme especificações e exigências do edital.

VALOR TOTAL HOMOLOGADO DA COMPRA: R\$ 4.830.000,00

Nome ou razão social do fornecedor: PTLIS SERVICOS DE TECNOLOGIA E ASSESSORIA TECNICA L

Qtd

Item 1: 400 Licença por servidor

- R\$ 8.932,25 (Un) | R\$ 3.572.900,00 (Total)



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

Item 2: 20 Licenças para cluster kubernetes

- R\$ 37.218,00 (Un) | R\$ 744.360,00 (Total)

Item 3: 200 Licenças para SO cliente

- R\$ 1.488,70 (Un) | R\$ 297.740,00 (Total)

Item 4: Serviço de configuração inicial do ambiente

- R\$ 215.000,00 (Total)

Prazo: 36 meses

Edital nº 90006/2024

Id contratação PNCP: 37115375000107-1-000045/2024

Fonte: Compras.gov.br

Órgão: MINISTERIO DO MEIO AMBIENTE

Unidade compradora: 440075 - SERVICO FLORESTAL BRASILEIRO

Objeto: O objeto da presente licitação é o registro de preço para a contratação de solução integrada de segurança, englobando microssegmentação de rede e segurança de borda para usuários e aplicações, web e nuvem, para o Serviço Florestal Brasileiro (SFB), para o Instituto Brasileiro de Recursos Naturais Renováveis e Meio Ambiente (IBAMA) e para o Ministério da Agricultura e Pecuária (MAPA) com implantação, garantia de assistência técnica e transferência de conhecimento, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

VALOR TOTAL ESTIMADO DA COMPRA: R\$ 5.088.573,63

Qtd

Item 1: 545 servidores

- R\$ 3.231,27 (Un) | R\$ 1.761.042,15 (Total anual)

Item 2: 6.747 estações de trabalho

- R\$ 451,74 (Un) | R\$ 3.047.889,78 (Total anual)

~~Item 3: 270 usuários - Solução de proteção de usuários e controle de dados em nuvem~~

- ~~• R\$ 1.035,71 (Un) | R\$ 279.641,70 (Total anual)~~

~~*item 3 não faz parte da contratação pretendida pela ALESP*~~

Prazo: Anual



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

6. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Com base na análise comparativa das soluções disponíveis, o cenário que atende às necessidades apresentadas neste estudo é o de contratação de solução de microssegmentação em modelo SaaS, por meio de appliances virtuais com suporte técnico garantido durante o período contratual. Treinamento oficial para a equipe técnica e horas de projetos sob demanda também fazem parte do escopo dessa contratação.

A solução a ser adquirida deve apresentar capacidade de segmentação granular do tráfego de rede, permitindo a criação de políticas de segurança baseadas em identidade, aplicação e contexto, com visibilidade detalhada e controle rigoroso das comunicações entre cargas de trabalho e dispositivos. Deve possibilitar a automação da orquestração de políticas, integração com ferramentas de segurança existentes e geração de relatórios de auditoria para rastreabilidade e conformidade.

A contratação do serviço em modelo SaaS visa garantir a escalabilidade, atualização contínua e alta disponibilidade da plataforma, além de suporte técnico especializado para implementação, operação e manutenção da solução de microssegmentação na infraestrutura corporativa, assegurando a proteção efetiva dos ativos digitais contra movimentações laterais e ameaças internas.

ITEM	Descrição	Qtd	Unidade
FASE 1 – Planejamento, Implantação e Transição (Entregas por Escopo)			
1	Plano de Implantação	1	Serviço
2	Solução de Microssegmentação para Servidores, Desktops e Notebooks – Licenças de 24 meses	2.500	Licenças
3	Implantação da Solução	1	Serviço
4	Operação assistida	1	Serviço
5	Capacitação Técnica na Solução	6	Vagas
FASE 2 - Suporte e Evolução (Serviço Continuado e Sob demanda)			
6	Serviço Continuado de Suporte e Manutenção	21	meses
7	Horas de projeto sob demanda	300	Horas



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

7. ESTIMATIVA DE QUANTIDADES

- A solução deverá ser dimensionada de forma a atender um ambiente com as seguintes características:

Tipo de Ativo	Qtd
Servidores Físicos "Bare metal"	10
Máquinas Virtuais "Virtual Machines"	260
Contêineres "Containers"	80
Desktops	1.850
Notebooks	300
TOTAL	2.500



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

8. ESTIMATIVA DE VALOR

Observações:

- As contratações públicas análogas, apresentadas no capítulo “5. Alternativas Possíveis”, variam em relação aos tipos de licenças de agente:
 - PRODEMG: menciona apenas licenças para “servidores”;
 - PRODEB: inclui licenças para “servidores” e “contêineres”;
 - MPSC: contempla licenças para “servidores”, “contêineres” e “estações de trabalho”;
 - SFB/MAPA: especifica licenças para “servidores” e “estações de trabalho”, mas devendo suportar a segmentação de ambientes em “contêineres”.
- Na tabela a seguir estão relacionados os valores encontrados, bem como um Preço Médio Unitário para um licenciamento de 24 meses, obtido com o seguinte método:
 - Converteu-se o valor dos contratos para 24 meses (dividindo-se pela quantidade de meses do respectivo contrato e, em seguida, multiplicando-se por 24);
 - Dividiu-se pela respectiva quantidade de licenças a fim de obter o valor unitário;
 - Calculou-se a média de preço para cada tipo de agente (“servidores”, “contêineres” e “estações de trabalho”) com base nos preços de cada processo de contratação pesquisado.
- Os custos dos serviços de Implantação, Capacitação Técnica, Suporte e Manutenção e Horas de projeto sob demanda em alguns casos estão inclusos no próprio licenciamento da solução ou não são requeridos nessas contratações.
- Observando-se que os custos dessas contratações são majoritariamente do licenciamento da solução (mais de 95% do valor) e que, nessa fase de ETP busca-se tão somente uma **ESTIMATIVA DE VALOR**, considerou-se apenas os preços médios de licenciamento para estimar o valor da contratação pretendida pela ALESP.



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

PREÇO MÉDIO UNITÁRIO BASEADO EM CONTRATAÇÕES PÚBLICAS ANTERIORES

ITEM	Descrição	Edital nº 201/2025 PRODEMG 24 meses		Edital nº 01/2025 PRODEB 36 meses		Edital nº 17/2024 MPSC 36 meses		C
		Qtd	Valor	Qtd	Valor	Qtd	Valor	
	FASE 1 – Planejamento, Implantação e Transição (Entregas por Escopo)							
1	Plano de Implantação	X	X	X	X	X	X	
2	Solução de Microsegmentação para Servidores, Desktops e Notebooks – Licenças de 24 meses	-	-	-	-	-	-	
2.1	Servidores	1.000	R\$ 8.108.000,00	500	R\$ 6.981.660,00	400	R\$ 3.572.900,00	5
2.2	Contêineres	X	X	50	R\$ 2.204.676,00	20	R\$ 744.360,00	
2.3	Estações de Trabalho	X	X	X	X	200	R\$ 297.740,00	6.
3	Implantação da Solução	X	X	X	R\$ 325.430,00		R\$ 215.000,00	
4	Operação assistida	X	X	X	X	X	X	
5	Capacitação Técnica na Solução	X	X	4	R\$ 78.540,00	X	X	
	FASE 2 - Suporte e Evolução (Serviço Continuado e Sob demanda)							
6	Serviço Continuado de Suporte e Manutenção	X	X	X	X	X	X	
7	Horas de projeto sob demanda	X	X	X	X	X	X	
TOTAL			R\$ 8.108.000,00		R\$ 9.590.306,00 (95,8% licença)		R\$ 4.830.000,00 (95,5% licença)	



ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO

ESTIMATIVA DE VALOR BASEADA NO PREÇO MÉDIO DE CONTRATAÇÕES PÚBLICAS ANÁLOGAS

ITEM	Descrição	Qtd	Unidade	Peço Unitário	Preço Total
FASE 1 – Planejamento, Implantação e Transição (Entregas por Escopo)					
1	Plano de Implantação	1	Serviço	X	X
2	Solução de Microsegmentação para Servidores, Desktops e Notebooks – Licenças de 24 meses	2.500	Licenças	-	-
2.1	Servidores	270	Licenças	R\$ 7.457,73	R\$ 2.013.587,10
2.2	Contêineres	80	Licenças	R\$ 27.103,84	R\$ 2.168.307,20
2.3	Estações de Trabalho	2.150	Licenças	R\$ 947,98	R\$ 2.038.157,00
3	Implantação da Solução	1	Serviço	X	X
4	Operação assistida	1	Serviço	X	X
5	Capacitação Técnica na Solução	6	Vagas	X	X
FASE 2 - Suporte e Evolução (Serviço Continuado e Sob demanda)					
6	Serviço Continuado de Suporte e Manutenção	21	meses	X	X
7	Horas de projeto sob demanda	300	Horas	X	X
PREÇO GLOBAL ESTIMADO					R\$ 6.220.051,30

e manutenção) não representam parcela significativa do valor global da solução, ficando responsáveis por aproximadamente 8%, enquanto o licenciamento concentra cerca de 92% do custo total.

350 servidores - 24 meses
2.100 estações de trabalho - 24 meses

Item	Descrição	Qtde	Valor unitário	Valor total 24 meses
1	Illumio Zero Trust Segmentation Platform Subscrição anual Licenças de microssegmentação para 350 dispositivos de rede (servidores) e 2100 estações de trabalho	2	R\$ 4.308.200,00	R\$ 8.616.400,00
2	Serviços de planejamento de implementação, implementação, operação assistida, suporte e treinamento	1	R\$ 770.000,00	R\$ 770.000,00
valor total				R\$ 9.386.400,00

Observou-se ainda que o valor obtido via consulta ao fornecedor apresentou-se superior ao valor estimado a partir dos preços médios das contratações públicas análogas. Essa diferença é esperada, considerando que cotações isoladas tendem a refletir preços de tabela, enquanto processos concorrenciais costumam gerar redução de valores em razão da disputa entre fornecedores. Também podem influenciar fatores como variação cambial, políticas comerciais distintas por órgão e oscilações periódicas no mercado de soluções importadas de segurança cibernética.

Diante desse cenário, optou-se por adotar, como estimativa final de valor deste ETP, a média aritmética simples entre:

- o valor estimado com base no preço médio das contratações públicas análogas, e
- o valor obtido por meio da consulta direta ao fornecedor.

Esse método reduz a probabilidade de superestimar ou subestimar o valor final e reflete de maneira equilibrada tanto o comportamento histórico das contratações públicas quanto a realidade atual de mercado observada na consulta direta.



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

A média resultante representa, portanto, uma estimativa prudente, realista e tecnicamente fundamentada, adequada para subsidiar o planejamento da futura contratação

Estimativa Final de Valor

Considerando:

- a) o valor médio obtido a partir das contratações públicas análogas pesquisadas, no montante de R\$ 6.220.051,30, e
- b) o valor decorrente da consulta direta a fornecedor, equivalente a R\$ 9.386.400,00,

adotou-se, como método de estimativa final, a média aritmética simples entre ambos os valores. Esse procedimento busca conciliar o comportamento histórico dos preços praticados no âmbito da Administração Pública com a realidade de mercado observada na cotação atual, evitando tanto superestimativas quanto subestimativas do custo total da solução.

Dessa forma, o valor estimado para a contratação é de:

R\$ 7.803.225,65

Valor considerado adequado, prudente e tecnicamente fundamentado para balizar as fases subsequentes de planejamento da contratação.

9. JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

A presente contratação contempla uma solução integrada de microssegmentação de rede, composta por licenciamento de software, serviços de implantação, capacitação técnica, operação assistida, suporte técnico, manutenção e horas de projeto sob demanda. Esses componentes são tecnicamente interdependentes e compõem um único projeto de segurança de rede, cuja efetividade depende da entrega coordenada e contínua de todas as partes.

A fragmentação da contratação em múltiplos lotes poderia comprometer:



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- A coerência técnica da solução;
- A responsabilidade unificada pela entrega e suporte;
- A gestão eficiente do contrato, dificultando o acompanhamento e a fiscalização;
- A continuidade operacional, especialmente nas fases de operação assistida e suporte técnico.

Além disso, o agrupamento em lote único está em conformidade com os princípios da eficiência, economicidade e padronização.

Dessa forma, a contratação em lote único é a forma mais adequada para garantir a entrega integrada, segura e eficaz da solução de microssegmentação, assegurando a qualidade técnica, a continuidade dos serviços e a economicidade do processo.

10. PROVIDÊNCIAS A SEREM ADOTADAS ANTES DA CELEBRAÇÃO DO CONTRATO

Não identificado nenhuma providência a ser adotada.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não identificado nenhuma contratação correlata e/ou interdependente.

12. POSSÍVEIS IMPACTOS AMBIENTAIS E AÇÕES MITIGATÓRIAS

A solução SaaS contribui para redução de consumo energético local, por não exigir infraestrutura física adicional, de modo que não se fez observar a existência de possíveis impactos ambientais negativos a serem mitigados.

13. RESULTADOS PRETENDIDOS

- Fortalecer os serviços *core* de rede para minimizar a existência de falhas de serviço frequentemente utilizadas como janelas de oportunidades para invasão ou vazamento de dados;



ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO

- Proteção de sistemas hospedados com segmentação de acessos e restrição de exposição;
- Incorporação de segurança de rede como requisito nativo dos sistemas desde o desenvolvimento.
- Redução do impacto de falhas, mantendo a continuidade de serviços não afetados.
- Controle granular baseado em identidade, função e contexto de risco.
- Geração de logs completos de comunicação leste-oeste para auditoria.
- Contenção automatizada de ameaças, isolamento de workloads e resposta rápida.
- Mapeamento em tempo real de fluxos e sistemas conectados.
- Maior confiabilidade da rede corporativa;
- Ter visibilidade em tempo real dos dispositivos conectados à rede corporativa e conseguir, mesmo com um parque de ativos de rede de múltiplos fabricantes, aplicar verificação de conformidade em cada dispositivo que tente se conectar;
- Melhorar o desempenho de todo o ecossistema de segurança cibernética, reduzindo o tempo e o custo da resposta a ameaças por meio de automação e compartilhamento de dados em tempo real com a utilização de APIs;
- Visibilidade e bloqueio de ataques nos serviços que sustentam a rede corporativa;
- Descoberta eficiente de fluxos de rede, contribuindo para a eficiência e segurança dos serviços de TI;
- Comunicação segura e segmentada entre dispositivos e aplicações na rede corporativa.

14. CONCLUSÃO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA ATENDIMENTO DA NECESSIDADE – DECLARAÇÃO DE VIABILIDADE

Diante do exposto, a equipe entende que a contratação em modelo SaaS de solução Microsegmentação de rede é a opção mais adequada e uma alternativa viável para que a Alesp possa atingir seus objetivos de negócios, assim como permite a manutenção de um ambiente disponível e seguro para os usuários, aumentando a segurança das informações e garantindo a continuidade dos negócios.



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

Análise de Riscos

Evento 1

Falta de capacidade técnica da empresa contratada.

Ação preventiva	Exigir qualificação econômico-financeira da contratada, regularidade fiscal e trabalhista, além de qualificação técnica. (Lei 14133/2021).
Responsáveis	Equipe de Planejamento de Contratação.
Ação de Contingência	Convocar o próximo colocado no processo de licitação nas mesmas condições do contrato firmado anteriormente.
Responsáveis	Gestor do Contrato

Evento 2

Interrupção da prestação de serviço – Incapacidade de execução total ou parcial dos serviços pela CONTRATADA (descumprimento de cláusulas contratuais, falência da empresa contratada e outras formas de suspensão ou cancelamento contratual).

Ação preventiva	Estabelecer no Planejamento da Contratação sanções e penalidades para os atrasos na entrega dos serviços contratados. Definir no Planejamento da Contratação indicadores de desempenho para medir a qualidade dos serviços contratados e estabelecer sanções e penalidades para o descumprimento dos Acordos de Nível de serviço. Estabelecer no Planejamento da Contratação multas severas, além de outras punições nos casos de descontinuidade dos serviços.
Responsáveis	Equipe de Planejamento de Contratação.



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

Ação de Contingência	Aplicar sanções e penalidades nos casos de atraso na entrega dos serviços contratados. Acompanhar os indicadores de desempenho e aplicar sanções/penalidades quando a qualidade dos serviços contratados não atender os níveis de serviços exigidos. Aplicar multas severas, além de outras punições nos casos de descontinuidade dos serviços.
Responsáveis	Gestor do Contrato

Evento 3	
Subutilização da solução contratada - Após a aquisição, a solução pode não ser utilizada em sua totalidade por falta de conhecimento técnico ou planejamento estratégico.	
Ação preventiva	Prever treinamento oficial e acompanhamento pós-implantação.
Responsáveis	Equipe de Planejamento de Contratação.
Ação de Contingência	Reavaliar uso e realizar reconfiguração orientada.
Responsáveis	Gestor do Contrato

Evento 4	
Atraso na implantação por falta de recursos do fornecedor - O fornecedor pode não alocar os recursos técnicos e humanos necessários no prazo acordado, causando atrasos na entrega da solução, comprometendo cronogramas de segurança e de continuidade de serviços.	



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

Ação preventiva	Estabelecer cronograma detalhado com SLA contratual
Responsáveis	Equipe de Planejamento de Contratação.
Ação de Contingência	Aplicar penalidades e solicitar reforço de equipe.
Responsáveis	Gestor do Contrato

Evento 5

Escopo pode ser modificado depois da finalização da entrega inicial- Experiência com a solução pode evidenciar a necessidade de modificações da entrega realizada sem o apoio do time de projeto, o que obriga a realizar modificações com equipe menos especializadas e com documentação não refletindo o estado atual da solução.

Ação preventiva	Conduzir levantamento de requisitos com o envolvimento de usuários-chave e áreas técnicas, prevendo possíveis cenários de uso.
Responsáveis	Equipe de Planejamento de Contratação.
Ação de Contingência	Contratação de horas de projeto sob demanda para customizações, integrações e ajustes conforme necessidades da contratante.
Responsáveis	Gestor do Contrato

Evento 6

Não renovação da contratação de microssegmentação – O encerramento da vigência das licenças sem renovação pode comprometer a política de segmentação da rede, elevando o risco de movimentação lateral de ameaças, diminuindo a visibilidade e ocasionando eventual descumprimento de requisitos regulatórios.



**ASSEMBLEIA LEGISLATIVA
DO ESTADO DE SÃO PAULO**

Ação preventiva	Planejar com antecedência mínima de 90 dias e promover a conscientização da alta administração sobre os riscos técnicos e operacionais envolvidos.
Responsáveis	Equipe de Planejamento de Contratação.
Ação de Contingência	Implantar controles compensatórios temporários (ACLs, firewall de borda, segmentação por VLAN) e priorizar a contratação emergencial de solução equivalente.
Responsáveis	Gestor do Contrato

Eliseu Camargo de Carvalho
Gestor de Divisão
Divisão de Redes e Segurança da Informação

Nilson Roberto Brito Dos Santos
Diretor de Departamento
Departamento de Tecnologia da Informação



Assinado por : ELISEU CAMARGO DE CARVALHO:35106471818

Data assinatura :25/11/2025 19:20:53

Assinado por : NILSON ROBERTO BRITO DOS SANTOS:13127027885

Data assinatura :26/11/2025 10:41:37