



HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
07/03/2025	1.1	Inicialização do artefato	Integrantes técnico e requisitante da EPCTIC
08/04/2025	1.2	Revisão do documento após análise	Integrantes técnico e requisitante da EPCTIC
02/06/2025	1.3	Revisão de alternativas válidas e inválidas	Integrantes técnico e requisitante da EPCTIC
06/10/2025	1.4	Revisão do documento após análise e adequação da especificação técnica	Integrantes técnico e requisitante da EPCTIC
04/12/2025	1.5	Finalização do documento	Integrantes técnico e requisitante da EPCTIC

*EPCTIC – Equipe de Planejamento da Contratação de TIC

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. 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).

O presente Estudo Técnico Preliminar visa proporcionar à escolha da melhor solução possível em termos de eficácia e efetividade, que atenda às necessidades de negócio que motivaram a demanda, e que seja economicamente viável, fornecendo informações necessárias para subsidiar os demais artefatos para o processo de contratação, em consonância ao Decreto nº 44.330 de 16 de março de 2023, que regulamenta a Lei nº 14.133/2021, de 1º de abril de 2021, que estabelece normas gerais de licitação e contratação para as Administrações Públicas Diretas, Autárquicas e Fundacionais da União, dos Estados, do Distrito Federal e dos Municípios, e normativos correlatados.

O art. 269-A do referido Decreto determina a adoção da regulamentação editada pela União sobre as contratações de bens e serviços de tecnologia da informação, de modo que se utilizou a Instrução Normativa SGD/ME nº 94/2022 e outros para fundamentar e nortear o planejamento das contratações de soluções Tecnologia da Informação e Comunicação - TIC na Polícia Civil do Distrito Federal - PCDF.

Documento elaborado pelos integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação, em observância e atendimento aos critérios do art. 11 da IN SGD/ME nº 94/2022.

Em consulta aos Catálogos de Soluções de TIC com condições padronizadas, definidos pela Órgão Central do SISP e disponibilizados no site do Governo Digital, verifica-se que abrangem licenciamento de software, tendo sido publicados os catálogos da Microsoft, Oracle, Qlik, Esri, Google, Adobe, VMWare, RedHat, Broadcom e Autodesk, até o momento da consulta. Uma vez que o objeto do presente estudo é uma plataforma de monitoramento em fontes abertas focada em inteligência de ameaças digitais, deixou-se de utilizar os referidos catálogos.

Cumprir informar que o presente ETP não se enquadra nas hipóteses de elaboração facultada (art. 9, §9º, IN SGD/ME nº 94/2022) ou dispensada (art. 9, §10, IN SGD/ME nº 94/2022).

1. IDENTIFICAÇÃO DO DOCUMENTO

Categoria:	Contratação de TIC
Número do Protocolo PCDF:	1863792/2024 - DITEC
Número do Protocolo SEI:	00052-00026224/2024-94
Documento Referência:	Documento de Oficialização de Demanda - DFD 16 (148485604)
Assunto:	Contratação de serviços para fornecimento de Solução de Segurança para Microsegmentação, incluindo instalação, implantação, treinamento, garantia e manutenção por 12 meses .

2. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Requisitante:	Carlos Said Oiticica Bandeira	Matrícula:	78.156-8
E-mail:	said.bandeira@pcdf.df.gov.br	Telefone:	3207-5023
Integrante Técnico:	Tulio Andre Pereira De Oliveira	Matrícula:	1.716.240-8
E-mail:	tulio.andre@pcdf.df.gov.br	Telefone:	3207-5023
Integrante Administrativo:	Érika Renata Vieira Bueno	Matrícula:	64.546-X
E-mail Administrativo:	erika.bueno@pcdf.df.gov.br	Telefone:	3207-5147

3. DESCRIÇÃO DA NECESSIDADE

3.1. Contratação de empresa para fornecimento de Solução de Segurança para Microsegmentação de rede, incluindo instalação, implantação, treinamento, garantia técnica, por 12 (doze) meses.

3.2. Motivação/Justificativa:

3.2.1. A Polícia Civil do Distrito Federal (PCDF) é uma instituição que tem como atribuição a apuração das infrações penais e a investigação criminal, conforme a Constituição Federal e leis específicas. Para cumprir sua missão, a instituição precisa de tecnologia e equipamentos atualizados, capazes de garantir a eficiência e a eficácia de seus processos.

3.2.2. A Polícia Civil do Distrito Federal (PCDF) é uma instituição que tem como atribuição a apuração das infrações penais e a investigação criminal, conforme a Constituição Federal e leis específicas. Para cumprir sua missão, a instituição precisa de tecnologia e equipamentos atualizados, capazes de garantir a eficiência e a eficácia de seus processos.

3.2.3. Os objetivos estratégicos da PCDF incluem a modernização tecnológica, a otimização de processos, a valorização do servidor e a excelência na prestação de serviços. É importante destacar que, em meio a este contexto, a segurança da informação é um aspecto fundamental.

3.2.4. Diante de um cenário de evolução desafiador, onde os riscos de cibersegurança estão em ascensão, torna-se fundamental que a Instituição busque abordagens proativas que visam mitigar essas ameaças, aumentando sua resiliência cibernética.

3.2.5. As ameaças atuais, como ransomware e violações de dados, podem não ser barradas em sua totalidade com ferramentas tradicionais de prevenção, como as que são utilizadas atualmente pela PCDF.

3.2.6. As estratégias de ransomware estão em constante evolução visando burlar a detecção e os controles de segurança.

3.2.7. O objetivo dos ataques de ransomware é criar um mapeamento de todo o ambiente de redes. O trabalho é feito de modo lateral, movendo os invasores de uma máquina ou servidor para outro, utilizando credenciais roubadas para abrir portas dos sistemas, efetuando o sequestro dos dados. Quando os dados são sequestrados, é feito então o pedido de resgate para a recuperação.

3.2.8. A solução de microsegmentação é uma técnica avançada de segurança de rede cujo papel é o de dividir a rede em segmentos menores e mais isolados, denominados de microssegmentos. Cada segmento tem suas próprias políticas de segurança, controles de acesso e monitoramento, limitando a comunicação entre eles a apenas o que é estritamente necessário, dificultando assim a propagação de ameaças de um segmento para o outro.

3.2.9. Em caso de incidente de segurança da informação, como um ataque de ransomware ou violação de dados, a microssegmentação permite isolar a área afetada imediatamente, impedindo a propagação do ataque e permitindo uma recuperação mais eficiente do ambiente, fazendo com que aumente a resiliência da rede da PCDF.

3.2.10. O uso combinado de ferramentas tradicionais adotadas pela PCDF, como antivírus e firewall, junto com a solução de microssegmentação, também conhecida como segmentação de confiança zero (Zero Trust Segmentation), aumentará significativamente as chances de proteção bem sucedidas.

3.2.11. Diante dos cenários de riscos de ataques, a solução de microssegmentação por ser um processo de implementação de isolamento e segmentação da rede, passa a ser uma camada de segurança a mais, somando na contenção dos possíveis danos, contribuindo com a melhoria da maturidade dos controles de segurança, diminuindo a superfície de ataques maliciosos, criando redes lógicas virtuais, independentes da estrutura física, possibilitando o monitoramento do tráfego e a identificação de ataques maliciosos, aumentando a proteção essencial para a missão crítica da PCDF, além de melhorar a eficiência operacional e conformidade com regulamentos.

4. NECESSIDADES DE NEGÓCIO

4.1. A Polícia Civil do Distrito Federal conforme definido no Mapa Estratégico Corporativo –2024 a 2027, necessitará de ferramentas, pessoas e tecnologias adequadas para suportar o conjunto de atividades que necessita desempenhar visando atender a sociedade do Distrito Federal..

4.2. Nesse sentido, com vistas a garantir um serviço de qualidade à população do Distrito Federal, a Polícia Civil vem ao longo dos anos desenvolvendo e disponibilizando sistemas e soluções de Tecnologia da Informação e Comunicação cada vez mais eficientes aos cidadãos, seus usuários internos, bem como aos Órgãos parceiros como TJDF, Ministério Público, Detran/DF, SSP/DF, DPF, entre outros.

4.3. Para alcançar os objetivos acima descritos, a Instituição utiliza como balizadores o Plano Diretor de **Segurança da Informação-PDTIC e a Política de Segurança da Informação-PSI**, documentos estratégicos que estão alinhados entre si, buscando garantir o uso seguro, eficiente e eficaz da tecnologia da informação.

4.4. O Plano Diretor de Tecnologia da Informação e Comunicação da Polícia Civil do Distrito Federal–PDTIC/PCDF é o documento estratégico utilizado para planejar, organizar e direcionar as ações de Tecnologia da Informação e Comunicação em consonância com os objetivos estratégicos institucionais na PCDF, a fim de atender às demandas de alta qualidade dos serviços prestados à sociedade.

4.5. A **Política de Segurança da Informação da PCDF-PSI** foi publicada por meio da Resolução n.º 01 de 10 de agosto de 2022 visando estabelecer na estrutura organizacional da Instituição, princípios e diretrizes que visam manter a conformidade com as disposições legais vigentes para assegurar a confidencialidade, a disponibilidade e a integridade de suas informações.

4.6. No contexto orgânico da PCDF, a Divisão de Tecnologia – DITEC é responsável pelo processamento das Ocorrências e Inquéritos Policiais, Mandados de Prisão, Alvarás de Soltura, Registros de Identificação Civil e Criminal, além da automação de mais de 100 (cem) Unidades Policiais e a salvaguarda de informações relevantes e sigilosas que devem ser protegidas com a utilização de técnicas e equipamentos confiáveis capazes de prover a disponibilidade e a integridade das informações.

4.7. **No âmbito da DITEC, o Serviço de Segurança em Tecnologia da Informação - SSTI** tem como atribuição principal atuar na elaboração de planos e metas relacionadas à Segurança em Tecnologia da Informação em conformidade com o previsto pela Política de Segurança da Informação, assim como prestar auxílio na implantação, no monitoramento e na aplicação de melhorias desses recursos. Dentre as atribuições desse serviço, destacam-se:

4.7.1. Gerenciar, coordenar e executar as atividades institucionais da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR/PCDF (Portaria Nº220, de 18 de maio de 2023);

4.7.2. Realizar a análise de vulnerabilidades;

4.7.3. Realizar auditorias, levantamento e correlacionamento de dados dos ativos de TIC da PCDF;

4.7.4. Realizar gestão de riscos relacionados a TIC, sugerindo as melhores práticas;

4.7.5. Elaborar e /ou acompanhar a elaboração de relatórios de segurança da informação.

4.8. A infraestrutura de TI da Instituição tem sua rede corporativa composta atualmente por servidores de rede, Kubernetes, dispositivos de armazenamento, firewalls, switches e endpoints, sendo a segmentação da rede realizada por meio de VLANs e firewalls de perímetro.

4.9. Estudo e dados de organizações que foram vítimas de ataques cibernéticos mostram que as medidas adotadas pela Instituição, em alguns casos, foram insuficientes para impedir movimentos laterais de ameaças mais avançadas.

4.10. Com o crescimento do ambiente de TI e buscando aprimorar a segurança das informações que são de responsabilidade da PCDF, levando-se em conta o cenário de evolução desafiador, onde os riscos de *cibersegurança* estão em ascensão, tendo como alvos principalmente as organizações governamentais, torna-se fundamental que a Instituição busque abordagens proativas que visem mitigar ameaças, aumentando sua maturidade em resiliência cibernética.

4.11. De acordo com os dados publicados pelo Gabinete de Segurança Institucional da Presidência da República (GSI) somente no primeiro mês do ano de 2024 foram, em média, 32 ataques cibernéticos por dia contra órgãos do Governo.

4.12. Diariamente os noticiários reportam incidentes de segurança que acontecem por transposição de defesas de perímetro, conforme os exemplos listados abaixo, envolvendo Órgãos do Governo e seus prejuízos: <https://www.gov.br/mj/pt-br/assuntos/noticias/ataque-cibernetico-contra-sistemas-do-governo-federal-sera-apurado-pela-pf>; <https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2024-07/sistema-do-governo-federal-que-sofreu-ataque-virtual-volta-funcionar>; <https://oglobo.globo.com/brasil/noticia/2024/03/01/ataques-ciberneticos-contra-orgaos-do-governo-federal-crescem-em-janeiro-puxados-por-vazamentos-de-dados.ghtml>; https://securityleaders.com.br/hackers-promovem-ataque-ddos-contra-instituicoes-brasileiras-apos-bloqueio-do-x/?utm_campaign=sr_daily_030924&utm_medium=email&utm_source=RD+Station; Ataques a sistemas do governo se aproximam de marc... | VEJA (abril.com.br); ATUALIZADO: Linha do tempo destaca ataques mais recentes - Security Leaders

4.13. Os incidentes cibernéticos contra órgãos públicos podem causar graves danos, como atraso na prestação de serviços, indisponibilidade desses, além de vazamentos de dados e violações da privacidade e da Lei Geral de Proteção de Dados (LGPD). No caso da PCDF, a indisponibilidade dos serviços prestados ou o vazamento de dados podem causar danos irreparáveis para a Sociedade.

4.14. As ameaças atuais, como ransomware, violações de dados e ameaças persistentes avançadas, podem não ser barradas em sua totalidade por ferramentas tradicionais de prevenção (defesas de perímetro) como as que são utilizadas pela PCDF no momento.

4.15. As ameaças persistentes avançadas (APTs) são classes de ataque que, após conseguirem o acesso ao ambiente, se escondem, sem serem detectados, exfiltrando dados ou aguardando o momento oportuno para lançar um ataque ainda mais devastador. O objetivo desse tipo de ataque é tornar extremamente difícil a prevenção, a proteção, a detecção e a resposta a ataques subsequentes. Esse tipo de ataque tem como alvo entidades de alto valor, que possuem dados significativos ou confidenciais, sendo as organizações de segurança uma das mais frequentemente visadas.

4.16. As APTS se destacam das demais ameaças cibernéticas por sua sofisticação e complexidade, combinando técnicas avançadas com táticas sociais. São planejadas e executadas após extensa pesquisa e estudo sobre a superfície de ataque da vítima. Em sua fase de execução, seu principal objetivo é não ser detectado na rede pelo maior tempo possível, podendo durar semanas e até anos.

4.17. A detecção dessas ameaças atuais requer estratégia de segurança abrangente, englobando busca de ameaças em processos, cargas de trabalho, plataformas, segmentos, além de um monitoramento meticuloso de todo ambiente, com análise contínua do tráfego da rede de entrada e saída.

4.18. A falta de uma solução na Instituição que se proponha a fazer todos esses papéis pode dificultar as respostas oportunas e eficazes da equipe de resposta a incidentes.

4.19. Diante do exposto e visando mitigar essas ameaças, a PCDF necessita de soluções que monitorem o ambiente, além de implementar diferentes camadas de segurança, complementando as proteções que já são implementadas no ambiente atualmente.

4.20. O objetivo deste Estudo Técnico Preliminar é analisar e identificar a solução que melhor atenda à necessidade do Órgão no que diz respeito à melhoria da segurança das informações, buscando reduzir o risco de acidentes cibernéticos, aumentando a resiliência da rede de dados. É objetivo ainda deste estudo a demonstração da viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

4.21. Dentro deste contexto, por meio de estudos realizados, a solução de microssegmentação de redes se apresenta como uma solução eficaz para garantir a proteção e o controle granular de acessos dentro da rede. **Dentre os benefícios que esse tipo de solução trará para a PCDF estão:**

4.21.1. Isolamento de Sistemas Críticos;

4.21.2. Redução de superfície de ataque;

4.21.3. Resposta rápida a incidentes;

- 4.21.4. Conformidade com regulamentos e normas;
- 4.21.5. Auditoria e monitoramento;
- 4.21.6. Proteção de dados sensíveis;
- 4.21.7. Controle granular dos acessos;
- 4.21.8. Gestão de riscos;
- 4.21.9. Segurança proativa;
- 4.21.10. Redução de impacto em caso de brechas de segurança;
- 4.21.11. Facilidade na administração de redes complexas;
- 4.21.12. Melhoria no Desempenho da Rede;
- 4.21.13. Suporte à mobilidade e ao trabalho remoto;
- 4.21.14. Integração com outras tecnologias de segurança;
- 4.21.15. Continuidade operacional;
- 4.21.16. Visibilidade e controle granulares sobre o tráfego de rede;
- 4.21.17. Gerenciamento de políticas simplificado;
- 4.21.18. Apoio nas auditorias de Segurança da Informação e proteção dos dados;
- 4.21.19. Modernização das soluções de Segurança Cibernética, com o provimento de recursos compatíveis com o atendimento das demandas atuais da tecnologia;
- 4.21.20. Segurança de movimento lateral e
- 4.21.21. Aplicações críticas seguras.

5. NECESSIDADES TECNOLÓGICAS MÍNIMAS PARA O OBJETO

5.1. As necessidades tecnológicas, também conhecidas como requisitos da solução de tecnologia, descrevem as características de uma solução que atenda aos requisitos do negócio. A solução pretendida deve atender aos seguintes requisitos técnicos:

- 5.1.1. Deverá assegurar a microsegmentação da rede corporativa como medida para aumentar a segurança do ambiente.
- 5.1.2. Deverá permitir a visualização do fluxo de aplicativos – descobrir automaticamente os fluxos de aplicativos em toda a rede e mapear as cargas de trabalho até o nível do processo.
- 5.1.3. Deverá proteger o tráfego leste/oeste (movimentação lateral), reduzindo a superfície de ataque e os riscos associados ao movimento lateral no ambiente.
- 5.1.4. Deverá analisar de forma automatizada uma ameaça de ataque – Inteligência de ataque de alta fidelidade, incluindo ferramentas, táticas e fontes dos invasores.
- 5.1.5. Deverá possuir funcionalidades de Resposta a incidentes – Recomendações de isolamento e correção de ataques que aceleram a resposta a incidentes.
- 5.1.6. Deverá implementar camada de defesa contra ransomware tanto para o ambiente atual, quanto para futuras expansões.
- 5.1.7. Deverá permitir a descoberta de máquinas e aplicativos.
- 5.1.8. Deverá permitir a criação de grupos de segurança para cada uma das diferentes camadas de aplicativos (ou seja, servidores web/aplicativos/bancos de dados etc.).
- 5.1.9. Deverá permitir a criação de uma política rígida entre os diferentes grupos de segurança, de forma que apenas as portas necessárias para o bom funcionamento do aplicativo sejam abertas.
- 5.1.10. Deverá enviar as violações de políticas e incidentes de segurança detectados, em tempo real, para a solução de SIEM.
- 5.1.11. Deverá ser compatível com sistemas legados, garantindo que não haja interrupções nas operações.
- 5.1.12. Deverá garantir interoperabilidade com outras ferramentas de segurança já em uso pela Instituição.
- 5.1.13. Deverá ser escalável para suportar o crescimento futuro da Instituição, tanto em quantitativo de usuários quanto de novos sistemas e aplicativos.
- 5.1.14. Deverá desenvolver alto nível de desempenho mesmo com o aumento do tráfego e da complexidade das políticas de segmentação.
- 5.1.15. Deverá garantir abordagem de segurança que forneça proteção para aplicativos, a nível de processos, web e nuvem para usuários remotos.
- 5.1.16. Deverá assegurar a realização de testes de segurança e constante evolução do nível de proteção das soluções de endpoint e rede.
- 5.1.17. Deverá permitir a verificação de comportamento do tráfego em tempo real.
- 5.1.18. Deverá permitir que qualquer ajuste ou configuração das funcionalidades dos módulos da solução que requeiram integração com ferramentas externas seja realizado de forma nativa ou através do uso de APIs.
- 5.1.19. Deverão ser observados e aplicados minimamente, nos casos em que qualquer módulo da solução obrigatoriamente necessite ser hospedado ou utilize recursos em nuvem, os requisitos legais que constam no item 7.1 – Requisitos Legais.
- 5.2. As exigências acima se justificam com a busca de mitigar o risco de exposição indevida de informações ou de ataques que reduzam a disponibilidade dos Sistemas da PCDF, serviços estes que são indispensáveis para segurança do Distrito Federal.

6. RESTRIÇÕES TÉCNICAS

- 6.1. Não serão aceitas soluções que sejam “Forks” de projetos de software existentes, ou seja, versões derivadas que tenham sido modificadas a partir do código fonte original.
- 6.2. Essa restrição visa garantir a integridade, o suporte contínuo e a segurança da solução adotada.
- 6.3. O objetivo da restrição é assegurar que a solução implementada possa:
 - 6.3.1. Receber atualizações regulares e suporte oficial, minimizando riscos associados a vulnerabilidades de segurança e garantindo a continuidade operacional;
 - 6.3.2. Manter a compatibilidade com outros sistemas e padrões tecnológicos, evitando problemas de interoperabilidade que possam surgir a partir de versões modificadas de softwares originais;
 - 6.3.3. Estar em conformidade com as políticas de licenciamento e propriedade intelectual, assegurando que não ocorram infrações legais ou contratuais decorrentes do uso de versões não autorizadas ou modificadas de softwares.
- 6.4. Serão consideradas apenas as soluções que utilizem versões oficiais e não modificadas dos softwares, garantindo conformidade com os padrões estabelecidos e assegurando a qualidade e a confiabilidade da implementação.

7. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

7.1. Requisitos Legais

- 7.1.1. A contratada deverá se submeter à Política de Segurança da Informação (PSI) da PCDF, nos termos da Resolução N° 01 de 10 de agosto de 2022.
- 7.1.2. Conformidade Regulatória: Caso o contrato envolva solução que utilize computação em nuvem, a CONTRATADA deverá rigorosamente cumprir e comprovar as cláusulas de segurança estabelecidas na Norma de Gestão de Computação em Nuvem da PCDF, Seção III – Da Utilização e Contratação de Serviços em Nuvem, Art. 12. que solicita:
 - 7.1.2.1. Garantia por parte da CONTRATADA de que os serviços ofertados estejam alinhados à legislação brasileira, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo tanto das comunicações privadas, quanto dos registros das operações.
 - 7.1.2.2. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela PCDF deverão ser hospedados preferencialmente em território brasileiro,

com as exceções a isso sendo tratadas em procedimentos específicos.

7.1.2.3. No caso das exceções, as informações sobre as localizações geográficas onde os dados são armazenados, processados e transmitidos devem ser registradas para que seja possível determinar as entidades regulatórias e as jurisdições aplicáveis.

7.1.3. A CONTRATADA deverá assegurar que todos os serviços e soluções de computação em nuvem fornecidos estejam em conformidade com as com as normas e regulamentos aplicáveis ao setor de segurança pública, incluindo, mas não se limitando a Lei Nº 13.709/2018 - LGPD, o Marco Civil da Internet, normas de segurança da informação ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018.

7.1.4. Condições Contratuais: O contrato deve prever cláusulas claras sobre responsabilidades, garantias, níveis de serviço (SLAs) e, condições de renovação ou cancelamento.

7.1.5. Propriedade Intelectual e Dados: o contrato deve garantir que a PCDF mantenha a propriedade dos dados e que os mesmos estejam protegidos contra acessos não autorizados, inclusive pelo fornecedor da solução.

7.2. Requisitos de Suporte e Manutenção

7.2.1. O suporte técnico deverá ser prestado pelo período de 12 (doze) meses contados a partir da data de recebimento definitivo e contemplar a prestação dos serviços a seguir:

7.2.2. Para o suporte técnico a Contratada deverá disponibilizar uma central de atendimento, incluindo sítio na internet, telefone (preferencialmente 0800) e e-mail, para abertura de chamados para suporte e manutenção, consultas, envio de arquivos para análise, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

7.2.3. Os chamados de suporte técnico deverão ser apresentados em sítio na internet, permitindo à CONTRATANTE o acompanhamento/evolução das informações relacionadas ao histórico dos atendimentos.

7.2.4. Nas atividades relacionadas ao atendimento do suporte técnico deverá ser empregada a língua portuguesa falada e escrita do Brasil.

7.2.5. A solicitação de suporte técnico deverá contemplar o esclarecimento de dúvidas, orientações no uso do software, configurações, instalação/desinstalação de funcionalidades da ferramenta, além de solução de problemas detectados pela equipe técnica da CONTRATANTE.

7.2.6. As atividades relacionadas ao suporte técnico deverão ser realizadas por profissionais certificados pelo fabricante, em razão da complexidade dos serviços a serem prestados.

7.2.7. Não haverá limitação para o número de chamados técnicos.

7.2.8. As atualizações de versão que ocorrerem durante a vigência contratual, deverão ser fornecidas automaticamente, sem ônus adicional para a CONTRATANTE.

7.2.9. Os serviços de manutenção compreendem as manutenções preventivas e corretivas, de forma que a solução esteja sempre em condições de funcionamento.

7.2.10. A CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novos releases, a partir do recebimento definitivo pela contratante, durante o período de garantia.

7.2.11. Caso seja necessário substituir licenças equivalentes durante a vigência do Contrato, isso deverá ocorrer sem qualquer ônus para a CONTRATANTE.

7.2.12. Os serviços deverão contemplar a resolução de qualquer problema nas licenças e serviços descritos neste documento, sem nenhum ônus adicional para a CONTRATANTE.

7.3. Requisitos Temporais

7.3.1. A reunião inicial deverá ocorrer em, no máximo, 5 (cinco) dias úteis após a assinatura do Contrato.

7.3.2. As licenças da solução ofertada deverão ser disponibilizadas à CONTRATANTE em no máximo 15 (quinze) dias corridos, podendo ser prorrogado por igual período caso haja justificativa plausível, a partir do recebimento da Ordem de Fornecimento de Serviço.

7.3.3. Todos os eventos de trabalho que envolvam participação de integrantes da CONTRATADA em ambiente da CONTRATANTE, tais como manutenção corretiva de software, deverão ser realizadas em regime 24x7, salvo acordo entre as partes.

7.3.4. Os esclarecimentos solicitados pela fiscalização do contrato deverão ser prestados imediatamente pela CONTRATADA.

7.3.5. A CONTRATADA deverá atender aos chamados técnicos de acordo com o item níveis mínimos de serviço exigidos no Termo de Referência.

7.3.6. O direito de atualização e suporte técnico das licenças, prestado diretamente pelo fabricante, deverá ser de 12 (doze) meses, contados do recebimento definitivo da solução.

7.3.7. A CONTRATADA deverá prover garantia de 12 (doze) meses, contados do recebimento definitivo da solução.

7.3.8. O treinamento será efetuado em até 30 dias a contar emissão do TRD – Termo de Recebimento Definitivo

7.4. Requisitos de Segurança da Informação e Privacidade

7.4.1. A CONTRATADA compromete-se, tanto em nome próprio quanto de seus colaboradores, a observar e cumprir rigorosamente todas as políticas, normas e procedimentos de segurança da informação, mantendo total conformidade com os normativos vigentes na CONTRATANTE, bem como com aqueles que possam ser estabelecidos durante a vigência do contrato.

7.4.2. Deverá ser firmado TERMO DE CONFIDENCIALIDADE E MANUTENÇÃO DE SIGILO entre a CONTRATADA e a CONTRATANTE, conforme modelo em anexo no Termo de Referência.

7.4.3. O TERMO DE CONFIDENCIALIDADE E MANUTENÇÃO DE SIGILO deverá ser assinado pelo representante legal da CONTRATADA, após a assinatura do contrato, em que se responsabiliza pela manutenção de **sigilo e confidencialidade** das informações a que possa ter acesso em decorrência da contratação.

7.4.4. A CONTRATADA deverá apresentar, para cada representante, empregado ou colaborador que vier a executar atividades referentes ao objeto da contratação, TERMO DE CIÊNCIA, conforme modelo em anexo no Termo de Referência, em que seus profissionais declaram estar cientes das responsabilidades pela manutenção de sigilo e confidencialidade.

7.4.5. A CONTRATADA deverá assumir total responsabilidade por todas as informações, documentos e especificações técnicas acessadas por seus representantes, empregados e colaboradores, no decorrer de todas as fases da execução dos serviços, devendo ser consideradas, em todo o tempo, como estritamente **confidenciais**. Fica proibida sua reprodução, utilização ou divulgação a terceiros, cabendo à CONTRATADA garantir a preservação total do **sigilo** das informações obtidas em função dos serviços prestados, em conformidade com o Termo de Compromisso e Manutenção de Sigilo e com os Normativos de Segurança da Informação.

7.4.6. A CONTRATADA deverá ser responsável por qualquer transferência ou remanejamento de seus colaboradores diretamente envolvidos na execução dos serviços objeto da contratação. Caso isso ocorra, a CONTRATANTE deverá ser comunicada com antecedência mínima de 5 (cinco) dias úteis, sendo obrigação da CONTRATADA providenciar a revogação de todos os privilégios de acesso às informações e recursos da CONTRATANTE.

7.4.7. Os profissionais da CONTRATADA que necessitem ter acesso às instalações físicas ou ao ambiente de rede da CONTRATANTE deverão, além de assinar o TERMO DE CIÊNCIA, ter seus dados previamente apresentados à CONTRATANTE, para realização de cadastro e concessão das permissões necessárias.

7.4.8. Não será permitido, em hipótese alguma, a divulgação, cópia ou retirada de quaisquer dados que estejam nos sistemas e bases de dados da CONTRATADA para fins que não estejam estritamente relacionados à prestação dos serviços contratados.

7.5. Requisitos de Treinamento e Capacitação

7.5.1. Deverá ser fornecido treinamento oficial pelo fabricante em português, com duração mínima de 20 horas para cada turma alocada.

7.5.2. O treinamento deverá ser ministrado por profissional com certificação oficial do fabricante.

7.5.3. O treinamento ofertado deverá abordar todos os componentes da solução fornecida, devendo ainda estar de acordo com a utilização da solução instalada no ambiente da CONTRATANTE.

7.5.4. A CONTRATADA deverá prover treinamento para 5 (cinco) participantes, com 20 (vinte) horas de carga horária mínima, respeitando o limite de 4 (quatro) horas por dia, contemplando a utilização de todos os módulos da solução contratada.

7.5.5. O treinamento será efetuado em até 30 dias a contar emissão do TRD – Termo de Recebimento Definitivo.

- 7.5.6. Deverá utilizar como base a solução implementada na CONTRATANTE, visando facilitar os casos práticos.
- 7.5.7. O **treinamento** deverá ser realizado no horário compreendido entre 14h00 e 18h00, em dias úteis, podendo haver alteração, a critério da CONTRATANTE, em comum acordo com a CONTRATADA.
- 7.5.8. O treinamento deverá ser realizado presencialmente, nas dependências da CONTRATANTE, em data a ser definida em comum acordo com a CONTRATANTE.
- 7.5.9. A CONTRATANTE poderá excepcionalmente, a seu critério, aceitar que o treinamento seja realizado de forma remota.
- 7.5.10. A CONTRATANTE disponibilizará laboratório com computadores e acesso à internet para a realização do treinamento.
- 7.5.11. À exceção da disponibilização do laboratório, todas as despesas decorrentes do treinamento, tais como pagamentos aos instrutores, diárias, confecção do material didático, ferramentas, coffee break, etc., serão de exclusiva responsabilidade da CONTRATADA.
- 7.5.12. O treinamento provido pela CONTRATADA será submetida à aprovação por parte dos alunos, conforme ficha de avaliação, item 7.5.18.
- 7.5.13. Caso o treinamento seja avaliado como INSATISFATÓRIA, será realizada novo treinamento para a turma, sem ônus à CONTRATANTE:
- 7.5.13.1. A critério da CONTRATANTE, o conteúdo poderá ser ajustado e/ou o instrutor substituído para sanar os problemas identificados.
- 7.5.13.2. O novo treinamento deverá acontecer segundo um novo calendário, a ser definido pela CONTRATANTE.
- 7.5.14. Todo o material utilizado para o treinamento deverá ser disponibilizado aos alunos em mídia eletrônica removível ou e-mail, em formatos padrão de mercado (PDF, DOC ou PPT). A CONTRATANTE se reserva o direito de reproduzir trechos do material didático utilizado no treinamento, desde que registradas as devidas fontes, para realizar capacitações internas a seus servidores e colaboradores.
- 7.5.15. A CONTRATADA deverá confeccionar certificado de participação do curso aos participantes que obtiverem no mínimo 75% de presença.
- 7.5.16. A CONTRATADA deverá enviar à CONTRATANTE a lista de presença, assinada pelo instrutor, em que seja comprovada a participação dos treinandos, por meio de suas assinaturas em cada dia da capacitação.
- 7.5.17. Para fins de comprovação dos serviços prestados, visando o faturamento, a CONTRATADA deverá encaminhar à CONTRATANTE, em até 5 (cinco) dias úteis após o encerramento da turma, os certificados e o documento de presença digitalizados.
- 7.5.18. **Avaliação do curso**
- 7.5.18.1. O treinamento de que trata este tópico será avaliado pelos técnicos da DITEC/DGI/PCDF, sendo que no caso de avaliação não satisfatória, deverá a CONTRATADA providenciar novo curso adequado às exigências e necessidades técnicas e didáticas para um aproveitamento satisfatório por parte dos técnicos inscritos;
- 7.5.18.2. O cálculo final da média de avaliação será feito pela soma das notas de cada uma das fichas de avaliação dividido pelo número de participantes. No caso de avaliação rejeitada (média final da avaliação inferior a 5), deverá a CONTRATADA providenciar novo curso adequado às exigências e necessidades técnicas e didáticas para um aproveitamento satisfatório por parte dos técnicos inscritos.
- 7.5.18.3. **Modelo de Ficha de Avaliação**

Marque com um "X" o conceito que melhor representa sua opinião sobre este curso:
1 – Deficitário; 2 – Regular; 3 – Bom; 4 – Muito Bom; 5 – Excelente

Item de Avaliação	Itens de Verificação	Notas				
		1	2	3	4	5
1	Metodologia utilizada					
2	Distribuição da programação					
3	Desempenho dos instrutores					
4	Adequação da carga horária					
5	Contribuição para a melhoria da qualidade do seu trabalho					
6	Adequação do conteúdo das aulas ao objetivo do curso					
7	Aulas práticas					
8	Participação pessoal					
9	Material audiovisual					
10	Instalações das aulas práticas					
Nota Final da Ficha de Avaliação (Soma da nota de cada item / 5)						

Registre:

Aspectos positivos:

Aspectos negativos:

Sugestões:

7.6. Requisitos Sociais, Ambientais e Culturais

- 7.6.1. A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa SLTI/MPOG, Instrução Normativa nº 01/2010, de 19 de janeiro de 2010.
- 7.6.2. A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução dos serviços, em consonância à Lei Distrital nº 4.774/2012, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens e na contratação de obras e serviços pelo Distrito Federal.
- 7.6.3. Deverá também estar aderente ao Plano de Logística Sustentável da PCDF, 3ª edição, vigente até 2027, disponível em: <https://www.pcdf.df.gov.br/institucional/gestao-estrategica/9128/pls>
- 7.6.4. É dever do CONTRATADO adotar na execução do contrato, práticas de sustentabilidade ambiental, a recepção de bens, embalagens, recipientes ou equipamentos inservíveis e não reaproveitáveis pelo Incra, práticas de desfazimento sustentável, reciclagem dos bens inservíveis e processos de reutilização que sejam aplicáveis ao objeto desta licitação.
- 7.6.5. A utilização de tecnologias de virtualização, as quais podem ser definidas como soluções computacionais que permitem a execução de vários sistemas operacionais e seus respectivos softwares a partir de uma única máquina física, gera benefícios como melhor aproveitamento da infraestrutura existente, a redução no consumo de energia elétrica e menor emissão de carbono.
- 7.6.6. Os serviços prestados pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo Governo do Distrito Federal e pela PCDF.
- 7.6.7. A CONTRATADA deve respeitar as Normas Brasileiras – NBR, publicadas pela ABNT, sobre resíduos sólidos.

- 7.6.8. Sem prejuízo aos demais critérios de sustentabilidade aplicados, a CONTRATADA deverá ainda observar os critérios estabelecidos na legislação ambiental.
- 7.7. Requisitos de Propriedade Intelectual e Titularidade para soluções de fornecimento de Software**
- 7.7.1. A solução ofertada deve ser estritamente proprietária, entendendo-se como tal o software cujo código-fonte integral não esteja:
- 7.7.1.1. Disponibilizado ao público em repositórios abertos (GitHub, GitLab, Bitbucket, SourceForge ou congêneres);
- 7.7.1.2. Distribuído, no todo ou em parte, sob licenças reconhecidas pela Open Source Initiative (OSI) ou por cláusulas de copyleft;
- 7.7.1.3. Veiculado publicamente, mesmo sem licenciamento formal, em regime de domínio público ou equivalente.
- 7.7.2. O licitante deverá comprovar a titularidade ou a posse de direitos exclusivos sobre a plataforma, apresentando ao menos um dos itens listados a seguir:
- 7.7.2.1. Certificado de registro ou depósito de software emitido pelo Instituto Nacional da Propriedade Industrial (INPI) ou órgão internacional equivalente;
- 7.7.2.2. Declaração formal, subscrita por representante legal, afirmando que:
- a) Detém todos os direitos autorais patrimoniais do produto;
- b) Nenhum componente crítico foi, em qualquer tempo, disponibilizado em repositórios públicos;
- c) O código-fonte não se encontra sob licenças open source nem contém trechos oriundos de projetos de livre distribuição.
- 7.7.2.3. Relação de cliente corporativo de porte equivalente ou superior à CONTRATANTE que utilize a mesma versão proprietária da plataforma há pelo menos doze (12) meses.
- 7.7.3. Constituirá causa de inabilitação a apresentação de propostas baseadas em:
- 7.7.3.1. Plataformas cujo núcleo funcional de microsegmentação (captura do tráfego, mapeamento do fluxo, definição de políticas, permissão e bloqueio de tráfego) seja derivado de projetos open source.
- 7.7.3.2. Ferramentas que, em sua atual versão, dependam de componentes copyleft indispensáveis ao funcionamento da microsegmentação da rede..
- 7.7.3.3. Reempacotamentos, forks, white-labels ou “Community Editions” de projetos open source, distribuídos sob licenças permissivas ou sem licenciamento formal.
- 7.7.3.4. Inclusão, em qualquer parte da solução, de trechos de código-fonte obtidos de repositórios públicos, ainda que sem licenciamento explícito ou sob domínio público.
- 7.7.4. Será admitido o uso de bibliotecas de sistema, sistemas operacionais, bancos de dados ou frameworks de uso geral licenciados como open source exclusivamente quando:
- 7.7.4.1. Tais componentes não integrarem o núcleo funcional da microsegmentação da rede (captura do tráfego, mapeamento do fluxo, definição de políticas, permissão e bloqueio de tráfego).
- 7.7.4.2. Não impuserem obrigações de copyleft ou de publicação de código ao software proprietário da CONTRATADA;;
- 7.7.5. A CONTRATADA deverá fornecer documentação técnica oficial comprovando que os componentes críticos da plataforma são mantidos exclusivamente pelo fabricante;
- 7.7.6. A CONTRATANTE reserva-se o direito de realizar auditoria técnica, a qualquer tempo, para verificar a conformidade do produto às exigências de propriedade intelectual previstas neste item. A constatação de violação acarretará rescisão contratual e aplicação das penalidades cabíveis, nos termos do art. 156 da Lei 14.133/2021.
- 7.8. Requisitos de Projeto e Implementação**
- 7.8.1. A CONTRATADA deverá entregar, instalar e configurar todo o sistema de gerenciamento da solução, tornando a solução operável e integrada com todos os equipamentos que compõem o ambiente tecnológico da PCDF.
- 7.8.2. Requisitos da Implantação:
- 7.8.2.1. Apresentação de cronograma de implantação;
- 7.8.2.2. Disponibilização de softwares dentro do prazo contratual;
- 7.8.2.3. Instalação e customização das configurações da solução;
- 7.8.2.4. Repasse de conhecimento da solução à equipe técnica da PCDF.
- 7.9. Requisitos de Garantia**
- 7.9.1. Todos os serviços entregues pela CONTRATADA deverão ser cobertos por garantia técnica durante 12 (doze) meses, tempo de vigência do contrato.

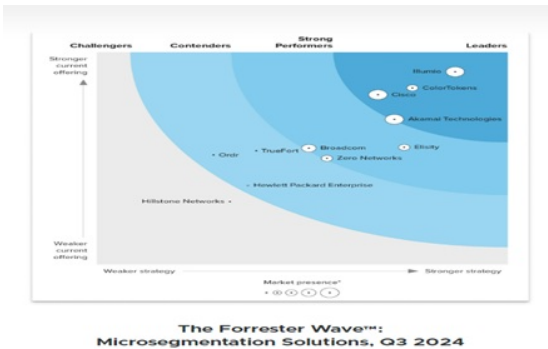
8. ESTIMATIVA DA DEMANDA

- 8.1. A tabela abaixo apresenta o detalhamento da demanda para a contratação de serviços para fornecimento de Solução de Segurança para Microsegmentação, incluindo instalação, implantação, treinamento, garantia e suporte técnico por 12 (doze) meses.

ITEM	DESCRIÇÃO	Unidade de Medida	QUANTIDADE
1	Fornecimento de Solução de segurança para microsegmentação de ambiente corporativo com licenciamento para Servidores	Solução	516
2	Fornecimento de Solução de microsegmentação de ambiente corporativo com licenciamento para Endpoints	Solução	5000
3	Fornecimento de Solução de microsegmentação de ambiente corporativo com licenciamento para Kubernetes	Solução	21
4	Serviço de Instalação da solução	Serviço	1
5	Serviço de Treinamento	Usuário	5

9. LEVANTAMENTO DE SOLUÇÕES

- 9.1. Na identificação e avaliação dos cenários possíveis para solução em questão, buscou-se parâmetros que ampliem a competitividade entre os licitantes, evitando critérios excessivos, restritivos e não justificados para a solução, além de balizadores, a exemplo de:
- 9.1.1. Especificações técnicas, quantidades, recursos orientados às necessidades de negócio, ou finalísticas da Instituição;
- 9.1.2. Aspectos relacionados à garantia da continuidade dos serviços prestados por meio da infraestrutura computacional;
- 9.1.3. Sustentabilidade ambiental e eficiência energética;
- 9.1.4. Garantias técnicas compatíveis ao ciclo de vida da solução;
- 9.1.5. Prazo de entrega previsível e compatível às necessidades finalísticas.
- 9.2. Estudo e análise de mercado**
- 9.2.1. Alinhado aos parâmetros supramencionados, foi realizada uma análise de mercado visando identificar as soluções de segurança cibernética disponíveis capazes de atender às necessidades da PCDF.
- 9.2.2. Em busca de soluções de microsegmentação foram realizadas buscas em mecanismos de pesquisa da internet, tendo sido encontrado o site da Forrester, ferramenta de pesquisa amplamente utilizada para embasar decisões de negócios, que mostra por meio de gráficos o mercado tecnológico e suas principais soluções em um lapso temporal. No contexto do estudo técnico, o uso da ferramenta facilitou a identificação das principais ferramentas de microsegmentação do mercado, conforme demonstrado abaixo:



9.2.3. De modo geral, as ferramentas ofertadas pelos diferentes fabricantes acima referenciados, operam de maneira similar, visando promover controles de segurança no nível de aplicativo para aumentar a visibilidade do tráfego e reduzir a superfície de ataque.

9.2.4. A análise de mercado indica que estão disponíveis soluções de segurança de microsegmentação tanto em modo on-premise, quanto em nuvem.

9.2.5. Complementarmente, são apresentados a seguir os aspectos relacionados ao mercado fornecedor, apontando suas principais características e especificidades relacionadas às compras de governo nesse segmento.

9.3. **Necessidade similar de outros**

9.3.1. A equipe de planejamento da contratação buscou junto ao mercado contratações com as seguintes características:

- 9.3.1.1. Escopo similar ao objeto
- 9.3.1.2. Similaridade de requisitos negociais e tecnológicos
- 9.3.1.3. Publicados recentemente e que foram atendidos com as soluções de mercado identificadas neste estudo técnico
- 9.3.1.4. O resultado foi o seguinte:

ID	PREGÃO	Análise
Serviço Florestal Brasileiro	90006/2024	Objeto similar ao pretendido
Companhia de Processamento de Dados do Estado da Bahia	01/2025	Objeto similar ao pretendido
MPSC	CT 022/2024/FERMP	Objeto similar ao pretendido - contratado em 11/2024, com licenciamento por 36

9.4. **Identificações das soluções**

9.4.1. Com o objetivo de encontrar soluções que atendam às necessidades acima elencadas, foram realizadas pesquisas em mecanismos de busca da internet. As soluções encontradas são as demonstradas abaixo:

D	Descrição da solução (ou cenário)
1	Contratação de empresa para fornecimento e instalação de solução de microssegmentação na rede da PCDF.
1A	Microssegmentação com suporte 24x7 e garantia (manutenção e suporte técnico), fornecida on-premise
1B	Microssegmentação com suporte 24x7 e garantia (manutenção e suporte técnico), fornecida em nuvem
2	Gerenciamento Manual via Firewall
3	Utilização de solução do Portal do Software Público Brasileiro

9.5. **Análise comparativa de soluções**

9.5.1. **Solução 1 – Contratação de empresa para fornecimento e instalação de solução de microssegmentação na rede da PCDF, suporte 24x7 e garantia (manutenção e suporte técnico).** A seguir serão apresentadas características gerais, comuns e compartilhadas tanto pela solução 1A quanto pela solução 1B. Em tópico subsequente, será realizada a comparação entre ambas.

9.5.1.1. A aquisição de uma solução de Microssegmentação oferece várias vantagens significativas que vão além da simples proteção contra ameaças cibernéticas, abrangendo também aspectos de conformidade, eficiência operacional, gestão de riscos, dentre outras:

9.5.1.1.1. **Aumento da Segurança**

9.5.1.1.1.1. Isolamento de Ameaças: permite o isolamento de aplicações e dispositivos em segmentos distintos, limitando a movimentação lateral de ameaças dentro da rede corporativa. No caso de comprometimento de um dos segmentos, a solução dificultaria o acesso do invasor aos demais.

9.5.1.1.1.2. Resiliência a Ameaças Avançadas: dificulta significativamente a execução de ataques avançados como APTs (Advanced Persistent Threats).

9.5.1.1.1.3. Proteção de Dados Sensíveis: No caso da PCDF que lida com dados altamente sensíveis, a microssegmentação assegura que somente usuários e sistemas autorizados tenham acesso a essas informações, reduzindo o risco de vazamentos de dados.

9.5.1.1.2. **Conformidade Regulatória**

9.5.1.1.2.1. Facilidade em atender as Normas de Segurança: ajudando a cumprir regulamentos de segurança da informação como a LGPD, ISO 27001, políticas internas da PCDF por meio de segmentações e controles de acesso.

9.5.1.1.2.2. Relatórios de Auditoria: a solução oferece visibilidade e controles, gerando logs e relatórios detalhados em caso de auditoria.

9.5.1.1.3. **Redução do Risco Operacional**

9.5.1.1.3.1. Contenção de Incidentes de Segurança: incidentes de segurança podem ser rapidamente contidos dentro de um segmento específico, minimizando o impacto no restante da rede e nas atividades da Instituição.

9.5.1.1.3.2. Redução da Superfície de ataque: A segmentação da rede em partes menores bem como a aplicação de políticas de segurança específicas reduz a superfície de ataques, dificultando as explorações de vulnerabilidades.

9.5.1.1.3.3. Proteção contra ameaças internas: limitação do acesso de usuários internos apenas aos recursos realmente necessários e permitidos, reduzindo o risco de ataques internos ou comprometimento acidental de sistemas críticos.

9.5.1.1.4. **Melhoria na visibilidade e Monitoramento**

9.5.1.1.4.1. Visibilidade do tráfego: a solução oferece visibilidade detalhada do tráfego em segmentos, permitindo que atividades anômalas ou suspeitas sejam identificadas com maior rapidez.

9.5.1.1.4.2. Monitoramento Contínuo: permite monitoramento contínuo do tráfego e das interações dentro da rede corporativa, facilitando detecção precoce de possíveis ameaças.

9.5.1.1.4.3. Elaboração de relatórios e análises em tempo real: permite a geração de relatórios e análises em tempo real sobre comportamento da rede, auxiliando na tomada de decisões mais rápidas e embasadas.

9.5.1.1.5. **Redução de Custos a longo prazo**

9.5.1.1.5.1. Prevenção de Incidentes: com a redução de ataques bem sucedidos e consequentemente se evitam custos significativos associados a resposta a incidentes, recuperação de dados e potenciais sanções regulatórias.

9.5.1.1.5.2. Otimização de recursos: com a automatização e a centralização da gestão de segurança, menos recursos serão necessários para manter a segurança da rede.

9.5.1.1.6. Fortalecimento da Confiança Pública

9.5.1.1.6.1. Reputação: a implementação de solução de microssegmentação na PCDF demonstra o compromisso da Instituição com a segurança e proteção dos dados sensíveis, fortalecendo sua imagem perante a sociedade e outros órgãos do governo.

9.5.1.2. Análise da Solução 1

9.5.1.2.1. Diante das principais soluções apresentadas nas pesquisas realizadas e visando avaliar e validar as entregas propostas pelas ferramentas, face às necessidades da Instituição expostas acima, a equipe técnica optou por realizar prova de conceito. Os testes foram realizados de forma satisfatória, tendo as ferramentas testadas mostrado resultados e relatórios adequados ao que se espera da solução, alinhados com as expectativas e necessidades da Instituição.

9.5.1.3. Prova de Conceito (PoC)

9.5.1.3.1. Como auxílio para o processo de avaliação técnica e com o objetivo de validar se a solução de microssegmentação atenderia aos requisitos estabelecidos pela equipe técnica do SSTI, foram realizadas 2 (duas) provas de conceito com soluções diferentes, a fim de testar a adequação da solução às necessidades da PCDF. As referidas provas de conceito tiveram como foco a validação da eficiência da solução no controle de tráfego interno, segmentação da rede, inventário de ativos, integração com as tecnologias existentes e mitigação de movimentação lateral de ameaças..

9.5.1.3.2. Ambiente de Testes: As PoCs foram realizadas em ambiente controlado e delimitado da infraestrutura da rede de dados da Instituição, contemplando:

9.5.1.3.2.1. Segmentação de redes internas em camadas de segurança, incluindo servidores críticos e estações de trabalho;

9.5.1.3.2.2. Aplicação de políticas de controle de acesso baseadas em perfis de usuários e dispositivos;

9.5.1.3.2.3. Levantamento de ativos e suas interligações;

9.5.1.3.2.4. Testes de movimentações laterais simuladas, visando avaliar a contenção de ataques;

9.5.1.3.2.5. Monitoramento de tráfego e geração de alertas de segurança em tempo real.

9.5.1.3.3. **Resultados obtidos:** Os testes demonstraram que as soluções foram eficazes na aplicação de políticas de microssegmentação, garantindo o isolamento de segmentos críticos da rede, impedindo a movimentação lateral em cenários simulados de ataques cibernéticos. Ademais, foi possível verificar, conforme relatório da equipe de segurança Instituição, que:

9.5.1.3.3.1. Eficiência na microssegmentação: as soluções foram capazes de isolar efetivamente segmentos da rede, aplicando políticas de acesso de maneira precisa e adaptável;

9.5.1.3.3.2. Desempenho: as soluções mantiveram desempenhos satisfatórios, sem impactos negativos no desempenho da rede corporativa;

9.5.1.3.3.3. Integração: as soluções se integraram de maneira eficiente com os sistemas de segurança já existentes na Instituição, tais como firewall, IDS e ferramentas de monitoramento da rede;

9.5.1.3.3.4. Facilidade de Gestão: as interfaces de gerenciamento testadas permitiram à equipe de segurança da PCDF criar, ajustar e administrar a solução de forma fácil e intuitiva.

9.5.1.3.4. Diante do exposto e com base nos testes de conceito realizados pela equipe técnica da PCDF, a solução de microssegmentação proposta, demonstrou atender positivamente aos requisitos de segurança, segmentação e controle, além de desempenho esperados, mostrando-se uma alternativa viável e recomendada pela equipe.

9.6. Análise comparativa de tipos de implementações possíveis da Microsegmentação

9.6.1. Visando aprimorar a proteção das informações, a Instituição editou normas de segurança da informação, incluindo a Resolução N.º 41/2024, que trata da Gestão de Computação em Nuvem.

9.6.2. A Norma traz em seu conteúdo a Seção III que versa sobre regras para a utilização e contratação de serviços em nuvem no âmbito da Instituição, conforme transcrito abaixo:

“Art. 11. No âmbito da PCDF, no papel disposto pelo inciso I do art. 10º, fica proibida a utilização ou contratação das categorias de serviços de Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS), exceto para o modelo de implantação de nuvem disposto no inciso III do art. 5º desta norma, sendo a PCDF a provedora do serviço, de acordo com o inciso II do art. 10º.”

§ 1º Em casos excepcionais, mediante solicitação a ser encaminhada ao DGI, será permitida a utilização ou contratação de soluções do tipo IaaS, PaaS ou SaaS informadas:

I – A Classificação das informações que serão tratadas;

II – Os riscos, as ameaças e as vulnerabilidades existentes;

III – A inexistência ou inviabilidade de alternativas que forneçam armazenamento local ou em nuvem privada ou interna à PCDF.

§ 2º Caso haja alternativas alinhadas ao Inciso III, o demandante deverá demonstrar a vantagem da alternativa proposta em relação à solução local ou em nuvem privada.

Art. 12. Após o recebimento de solicitação de utilização ou contratação de serviços de nuvem, deverá ser verificada, no mínimo, quão viável é a garantia de que os serviços ofertados estejam alinhados à legislação brasileira bem como os direitos à privacidade, à proteção dos dados pessoais e ao sigilo tanto das comunicações privadas quanto dos registros das operações. A exceção da comprovação de vantagem, conforme descrito no item anterior, não será concedido o acesso caso haja alternativa viável de solução instalada localmente ou em nuvem privada da PCDF.”

9.6.3. Ainda em referência ao normativo de Gestão de Computação em Nuvem, a Seção IV versa sobre o Armazenamento de Informações na Nuvem e em seu Art. 15 a seguinte condição:

“Art. 15. Dados, metadados, informações e conhecimentos produzidos ou custodiados pela PCDF deverão ser hospedados preferencialmente em território brasileiro, com as exceções a isso sendo tratadas em procedimentos específicos.

Parágrafo único. No caso das exceções tratadas no caput, as informações sobre localizações geográficas onde os dados são armazenados, processados e transmitidos devem ser registradas para que seja possível determinar as entidades regulatórias e as jurisdições aplicáveis.”

9.6.4. A partir dos critérios estabelecidos pela Norma de Gestão de Computação em Nuvem da PCDF e com base nos levantamentos e estudos realizados pela equipe técnica da SSTI, quanto aos tipos de implementação possíveis e ofertados pelas soluções disponíveis no mercado, descobriu-se que:

9.6.4.1. A solução de microssegmentação pode ser implementada tanto em ambiente on-premise (utilizando a infraestrutura local da Instituição) quanto em ambiente de nuvem (pública, privada ou híbrida), dependendo da infraestrutura e das necessidades da organização.

9.6.5. De acordo com os estudos realizados e com base nos dados e resultados obtidos na realização das provas de conceito e, ainda, buscando cumprir as regras impostas pelos normativos de segurança da informação da PCDF quanto à utilização e contratação de serviços em nuvem, os cenários avaliados são aqueles previamente enunciados, quais sejam, a contratação de solução de microssegmentação on-premise (solução 1A) e a contratação de solução de microssegmentação em nuvem. Os detalhes de cada um desses cenários serão apresentados a seguir:

9.6.5.1. **SOLUÇÃO 1A – Contratação de solução de Microsegmentação on-premises**

9.6.5.1.1. A solução de microssegmentação on-premise será instalada e configurada na infraestrutura física da Instituição, utilizando recursos da própria PCDF, tais como rede, links, storage, servidores, além de mão de obra especializada para a sustentação da solução em funcionamento.

9.6.5.1.2. Vantagens apresentadas:

9.6.5.1.2.1. Maior controle sobre a infraestrutura;

9.6.5.1.2.2. Baixa latência – tráfego fica dentro da própria rede local, sem dependência da internet e

9.6.5.1.2.3. Conformidade com os regulamentos da Instituição.

9.6.5.1.3. Desvantagens apresentadas:

9.6.5.1.3.1. Alto Custo - a solução exige equipamentos de rede robustos, firewall e suporte especializado;

9.6.5.1.3.2. Complexidade Operacional – requer monitoramento constante e reconfiguração manual da infraestrutura tornando-se uma solução rígida em caso de necessidade de mudanças, levando-se em conta a quantidade de endpoints que a Instituição possui;

- 9.6.5.1.3.3. Monitoramento e visibilidade – dificuldade na identificação de tráfego suspeito dentro dos segmentos;
- 9.6.5.1.3.4. Segurança – exigência de equipe especializada para configuração e monitoramento;
- 9.6.5.1.3.5. Gerenciamento – requer equipe de TI dedicada para ajustes constantes, o que pode ocasionar conflitos ou brechas de segurança;
- 9.6.5.1.3.6. Menos escalável - para expansão da solução poderão ser necessários novos investimentos em servidores e equipamentos.
- 9.6.5.2. **SOLUÇÃO 1B – Contratação de solução de Microsegmentação em Nuvem**
- 9.6.5.2.1. A solução de microsegmentação em nuvem será configurada dentro de infraestrutura de provedor de rede utilizando políticas de segurança baseadas em softwares.
- 9.6.5.2.2. **Vantagens apresentadas:**
- 9.6.5.2.2.1. Alta escalabilidade – permitindo a segmentação dinâmica sem necessidade de adição de qualquer tipo de hardware;
- 9.6.5.2.2.2. Automação – integração com inteligência artificial e aprendizado de máquina para resposta automática e mais eficaz contra ameaças.
- 9.6.5.2.2.3. Monitoramento e visibilidade – a possibilidade de integração com as ferramentas de vulnerabilidade tais como SIEM dentre outras, permitem identificar com maior rapidez o tráfego suspeito dentro dos segmentos da rede;
- 9.6.5.2.2.4. Gerenciamento de regras – se utiliza do uso de políticas dinâmicas baseadas em identidade e Zero Trust;
- 9.6.5.2.2.5. Infraestrutura – utiliza a infraestrutura de provedores com firewalls virtuais e políticas baseadas em identidade;
- 9.6.5.2.2.6. Facilidade de gerenciamento – o gerenciamento é realizado via em APIs e painéis de controle automatizados, permitindo implementação mais ágil, além de integração com as soluções de vulnerabilidades que se encontram em processo de aquisição pela Instituição.
- 9.6.5.2.3. **Desvantagens apresentadas:**
- 9.6.5.2.3.1. Dependência da nuvem – a segurança passa a ser compartilhada com o provedor, exigindo assim boas práticas de configuração;
- 9.6.5.2.3.2. Custo variável – pode ser barato no início, mas os custos de largura de banda e armazenamento podem aumentar;
- 9.6.5.2.3.3. Latência – dependendo da localização dos servidores, pode haver pequenas demoras no tráfego entre segmentos;
- 9.6.5.2.3.4. Conformidade: a implementação em nuvem necessitaria de autorização do DGI, após a comprovação de conformidade, por parte da empresa fornecedora da solução, com os requisitos que constam no Art. 11, § 1º.
- 9.6.5.2.4. **Diante dos estudos realizados pela equipe técnica da SSTI quanto às vantagens e desvantagens de cada tipo de implementação, as considerações são as seguintes:**
- 9.6.5.2.4.1. Em análise realizada quanto ao mercado, as empresas que fornecem esse tipo de solução oferecem tanto em modo on-premise quanto em nuvem, ficando claro que a escolha será exclusiva da PCDF.
- 9.6.5.2.4.2. Em termos de orçamentos e propostas de valores apresentados pelas empresas, o custo total final para a entrega da solução, seja ela on-premise ou em nuvem, é o mesmo. O que fará diferença no custo final será que, no caso da solução on-premise toda a disponibilização de infraestrutura (servidores, storages, softwares, firewall) para alocação e implementação será de responsabilidade da PCDF. No caso da solução em modo nuvem, todas as atribuições ficarão a cargo da empresa prestadora do serviço.
- 9.6.5.2.4.3. Dado que os valores dos dois tipos de solução não variam entre si, partiu-se para análise dos custos financeiros e operacionais que se apresentariam na instalação, manutenção, expansão e reconfiguração da solução on-premise, uma vez que a mesma requer que todos esses itens fiquem a cargo da Instituição.
- 9.6.5.2.4.4. O quadro apresentado abaixo demonstra de forma resumida os requisitos necessários para a implementação da solução de microsegmentação no modo on-premise.

ITEM	Descrição
Licenciamento de Software	Criação de novos servidores e uso de storage para suportar as cargas segmentadas.
Firewalls de Próxima Geração (NGFW)	Essenciais para criar segmentos de rede isolados.
Switches de Camada 3	Permitem segmentação via VLANs e ACLs.
Soluções SDN (Software Defined Networking)	Ex: VMware NSX, CISCO ACI – facilitam a segmentação dinâmica.
Software de Monitoramento e SIEM	Necessários para a análise do tráfego dentro dos segmentos
Consultoria e implementação	Treinamento para a equipe interna a fim de capacitá-los para a operação

- 9.6.5.2.4.5. Após a implementação, há custos recorrentes para manutenção e operação da solução e que ficarão a cargo da PCDF, conforme demonstrado abaixo:

ITEM	Descrição
Licenciamento de Software	VMware NSX
Equipe Especializada	Administração e manutenção da microsegmentação
Monitoramento e Resposta a Incidentes	SIEM, XDR, SOC (Security Operations Center)
Treinamento e atualização da Equipe	A fim de garantir boas práticas e conformidade
Suporte e Manutenção	Atualizações de hardware e software

- 9.6.5.2.4.6. Embora a infraestrutura da PCDF conte no momento com uma estrutura de servidores de rede e Storage robusta, o provisionamento desses recursos foram previstos para atender às altas demandas de processamento e armazenamento para sustentação dos serviços já prestados pela Instituição.
- 9.6.5.2.4.7. Dado que algumas das Unidades Internas da Instituição estão em processo de migração de seus dados e serviços para a estrutura disponibilizada pela Divisão de Tecnologia da PCDF, o que demanda ainda mais dos recursos acima descritos, a mobilização de outra parcela desses recursos para a instalação da solução de microsegmentação alteraria, oneraria e desviaria insumos que já haviam sido destinados à manutenção da qualidade dos serviços prestados à população do Distrito Federal.
- 9.6.5.2.4.8. Outro cenário que deve ser considerado é o que envolve os recursos humanos. A equipe de sustentação do Serviço de Segurança em Tecnologia da Informação é reduzida e se alterna entre variadas atividades que buscam a garantia da segurança da informação na Instituição.
- 9.6.5.2.4.9. A solução de microsegmentação on-premise requer administração e manutenção contínua dos segmentos de rede, aumentando a demanda operacional da equipe. Traz ainda como necessidade, o monitoramento constante para detecção de ameaças internas e falhas de configuração, gerando um gasto maior em termos de gestão de acessos e revisões de regra a fim de prevenir falhas de segmentação.
- 9.6.5.2.4.10. A responsabilidade por aplicar atualizações de segurança e corrigir vulnerabilidades ficará a cargo da equipe de sustentação. Por ser uma ação humana, falhas ou atrasos na atualização podem expor a rede a ataques e vulnerabilidades.
- 9.6.5.2.4.11. No que se refere à escalabilidade e adaptação, a solução on-premise apresenta limitações quanto a mudanças na infraestrutura, pois alterações na infraestrutura exigem planejamento prévio e tempo para implementação. Em contraste, soluções em nuvem permitem ajustes rápidos e flexíveis, facilitando a adaptação às necessidades do ambiente.
- 9.6.5.2.4.12. A configuração manual da segmentação pode levar a falhas de segurança ou permissão de acessos indevidos. Além do que, mudanças realizadas sem planejamento adequado podem gerar interrupções de serviços e downtime.
- 9.6.5.2.4.13. De acordo com as avaliações referentes à solução no modo on-premise, conclui-se que esse tipo de implementação, embora em conformidade com o normativo da PCDF, exigirá um grande esforço da equipe de TI, aumentando a demanda operacional, a complexidade da gestão, gastos futuros para expansão e os riscos inerentes ao

erro humano.

9.6.5.2.4.14. Dentro dos comparativos a partir dos estudos realizados, a microssegmentação em nuvem mostrou-se como uma alternativa mais flexível, escalável e econômica em comparação com a solução on-premise.

9.6.5.2.4.15. Em termos de redução dos custos operacionais, não há necessidade de hardware físico, gerando assim economia em manutenção e aquisição de servidores, softwares, firewalls e switches, pois todo o investimento e gerência de recursos é feito pelo provedor da nuvem.

9.6.5.2.4.16. A escalabilidade e elasticidade na solução em nuvem permitem o aumento de recursos de acordo com a demanda, evitando assim o desperdício, o sub ou o superdimensionamento. Essa característica traz como benefício a adaptação ágil às novas necessidades, sem custos desnecessários.

9.6.5.2.4.17. A configuração e manutenção da microssegmentação em nuvem são mais fáceis e podem ser automatizadas por meio de APIs. Além disso, utilizam interface única (gestão centralizada) para aplicação de políticas de segurança, requerendo assim, menor esforço humano para manutenção e trazendo maior eficiência operacional.

9.6.5.2.4.18. A nuvem permite uma segurança mais aprimorada, à medida que aplica princípios de Zero Trust, garantindo maior controle de acessos e menor risco de ataques.

9.6.5.2.4.19. As atualizações de segurança são automáticas, sendo aplicadas pelo provedor do serviço, garantindo maior proteção, sem que haja aumento de custo com hardware e equipe.

9.6.5.2.4.20. As análises e monitoramentos são avançados, utilizando inteligência artificial para detecção de ameaças, além de permitir conexão com soluções de terceiros para detecção de vulnerabilidades.

9.6.5.2.4.21. Comparativo entre a Microssegmentação On-premise X Nuvem

Fator	On-Premise	Nuvem
Investimento Inicial	Alto	Baixo
Escalabilidade	Limitada – para expansão pode ser necessária a compra/instalação de novos servidores e dispositivos de segurança, podendo levar semanas ou meses.	Ilimitada – conforme a necessidade da demanda, aumenta ou reduz recursos em minutos, sem necessidade de aquisição de hardware
Gerenciamento	Necessita equipe interna qualificada para monitoramento, atualizações e gerenciamento da segurança da rede.	Automatização e gestão centralizada, reduzindo erros humanos e otimizando processos. Aplicação de políticas de segurança de forma rápida e eficiente
Custo de Manutenção	Alto (hardware, suporte, atualização)	Médio (Licenciamento, uso variável)
Tempo de Implementação	Lento (configuração física)	Rápido (APIs e automação)

9.6.5.2.5. Em conclusão, após estudos e análises, levando-se em consideração inclusive as provas de conceito realizadas pela equipe do SSTI, a **microssegmentação em nuvem mostrou-se mais vantajosa em relação à versão on-premise principalmente em termos de custo**, escalabilidade, segurança e facilidade de gerenciamento.

9.6.5.3. SOLUÇÃO 2 – Gerenciamento Manual via Firewall

9.6.5.3.1. Este cenário possui inconvenientes que o tornam inviável tecnicamente, os quais podemos citar:

9.6.5.3.1.1. Segmentação limitada e insuficiente;

9.6.5.3.1.2. Risco de movimentação lateral;

9.6.5.3.1.3. Políticas de Segurança genéricas ou globais;

9.6.5.3.1.4. Falta de isolamento de Sistemas Críticos;

9.6.5.3.1.5. Falta de visibilidade da infraestrutura atual, com suas conexões e vulnerabilidades;

9.6.5.3.1.6. Limitações em análises de comportamento;

9.6.5.3.1.7. Maior risco de paralisação do ambiente em caso de ataques cibernéticos;

9.6.5.3.1.8. Atualizações manuais (mais demoradas e propensas a erros).

9.6.5.3.2. Fornecedores: Não há

9.6.5.3.3. A solução proposta seria continuar utilizando o firewall como ferramenta principal para a proteção contra ataques cibernéticos.

9.6.5.3.4. O firewall na estrutura de segurança da PCDF tem como função principal proteger o perímetro da rede, atuando como uma barreira entre a rede interna e as externas, filtrando o tráfego de entrada e saída de acordo com as regras de segurança pré-definidas pela equipe de segurança da Instituição.

9.6.5.3.5. Sua função é proteger a rede contra acessos não autorizados, impedindo que as tentativas de ataque cheguem à rede interna, bloqueando portas específicas, endereços IP maliciosos e protocolos inseguros, reduzindo de certa forma a superfície de ataque.

9.6.5.3.6. Embora seja indispensável para a segurança da rede, apresenta limitações relevantes quando as ameaças cibernéticas são mais sofisticadas, como os ataques persistentes que exploram vulnerabilidades desconhecidas ou os ataques internos, que surgem dentro da rede, táticas de engenharia social e movimentações laterais que podem contornar os controles deste firewall.

9.6.5.3.7. As ameaças que por ventura já tenham entrado na rede, caso o invasor obtenha sucesso ao passar pelo firewall, poderão se mover lateralmente explorando diferentes sistemas internos sem que seja detectado.

9.6.5.3.8. Além disso, o firewall não oferece visibilidade granular sobre o tráfego dentro da rede. Uma vez que o tráfego passou pelo perímetro, as interações internas entre servidores, aplicações e usuários não são monitoradas de maneira eficiente, podendo deixar lacunas onde atividades suspeitas possam ser executadas sem serem detectadas.

9.6.5.3.9. A ferramenta opera reativamente, detectando e bloqueando ameaças conhecidas ou tráfegos não autorizados, não conseguindo identificar comportamentos suspeitos ou prevenir ativamente ataques antes que eles aconteçam.

9.6.5.3.10. Além das situações mencionadas acima, o firewall pode apresentar dificuldade em lidar com a segurança de infraestruturas híbridas, distribuídas entre ambientes locais e na nuvem.

9.6.5.3.11. A tabela abaixo demonstra a diferença entre a segmentação com o uso de ferramentas tradicionais (uso apenas do firewall) X Microssegmentação:

Microssegmentação	Ferramentas tradicionais
Isolamento dos ativos de TI	Proteção de perímetro
Visibilidade Granular	Sem visibilidade
Acesso a cada servidor individualizado	Circulação livre entre máquinas dentro do perímetro
Acesso controlado de cada aplicação	aplicações vulneráveis a ataques direcionados
Controle de Tráfego entre cada servidor físico e virtual	Vulnerável à passagem de tráfego malicioso entre servidores
Controle de acesso entre as aplicações	Vulnerável a ataques originados de dispositivos de usuários comprometidos
Controle do comportamento das aplicações	Vulnerável a ataques diretos com técnicas de evasão

9.6.5.3.12. Considerando-se o uso atual de servidores de rede virtualizados, além de considerar a necessidade futura de projetos para uso de ambiente em nuvem na PCDF

e que o uso do firewall tradicional é mais eficaz em redes físicas, fica comprometida a capacidade de proteção desses ambientes, uma vez que exigem soluções mais dinâmicas.

9.6.5.3.13. Diante do que foi apresentado, considerando-se o aumento e a diversidade dos tipos de ataques cibernéticos externos e internos e visando tornar a proteção da rede da PCDF mais robusta, a equipe técnica entende que o firewall não é suficiente para desempenhar sozinho o papel de proteção da rede, apresentando lacunas significativas na detecção e prevenção de ataques avançados, como ameaças de dia zero, movimentação lateral na rede e ameaças internas, sendo necessário, diante do exposto, um complemento de outra tecnologia.

9.6.5.3.14. Sendo assim, a equipe técnica **não recomenda a adoção da alternativa de gerenciamento manual via firewall** em questão.

9.6.5.4. Solução 3 – Utilização de solução do portal de Software Público Brasileiro

9.6.5.4.1. O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e é compartilhado sem ônus no Portal do Software Público Brasileiro, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade.

9.6.5.4.2. Fornecedor: Portal de Software Público Brasileiro

9.6.5.4.3. O presente cenário tem o objetivo de analisar a aquisição junto ao Portal do Software Público Brasileiro para atender às necessidades da PCDF.

9.6.5.4.4. O principal objetivo do Portal é promover o desenvolvimento de um "ambiente colaborativo que não só reduz os custos do governo, mas também permite o desenvolvimento de artefatos tecnológicos" (Santanna, 2007). De acordo com Santanna, "o conceito de utilização livre de código fonte - que deve sustentar as sociedades modernas - é central para o Portal do Software Público Brasileiro. A Administração Pública brasileira precisava de um ambiente no qual diversos atores sociais fossem capazes de compartilhar suas soluções já testadas e aprovadas a fim de evitar, entre outros fatores, a sobreposição de custos com outras soluções que são similares às que já existem" (Santanna, 2007).

9.6.5.4.5. Além disso, o Portal colabora para a geração de emprego e renda, facilitando o contato entre pessoas que pretendem utilizar soluções informatizadas e aqueles que fornecem serviços. A rede estabelecida cria um complexo sistema de garantias econômicas, políticas e relações sociais que envolvem diversas esferas da sociedade. O software, neste contexto, não é apenas um produto, mas também um artefato por meio do qual seus criadores proporcionam novos referenciais de produção. Os atores neste cenário são simultaneamente produtores e consumidores, o que Tapscott & Williams definem como os prosumers" (Tapscott & Williams, 2007).

9.6.5.4.6. Conforme pesquisa no portal de software público Brasileiro, não se encontra disponível nenhuma solução de microsegmentação nos moldes até então descritos neste estudo.

9.6.5.4.7. Conclui-se pelos fatos expostos que não é possível adotar os softwares disponíveis no Portal de Software Público Brasileiro para atender às necessidades da PCDF.



CATÁLOGO DE SOFTWARE PÚBLICO

Resultado da pesquisa

PESQUISAR CATÁLOGO DE SOFTWARE

Todos

Software Público

micro segmentação

FILTRO

MAIS OPÇÕES

0 Software(s)

Exibir: 15

Ordenar por: Avaliação

Nenhum software encontrado. Tente outros filtros



CATÁLOGO DE SOFTWARE PÚBLICO

Resultado da pesquisa

PESQUISAR CATÁLOGO DE SOFTWARE

Todos

Software Público

zero trust

FILTRO

MAIS OPÇÕES

0 Software(s)

Exibir: 15

Ordenar por: Avaliação

Nenhum software encontrado. Tente outros filtros

CATÁLOGO DE SOFTWARE PÚBLICO

Resultado da pesquisa

PESQUISAR CATÁLOGO DE SOFTWARE

Todos

Software Público

segmentação

FILTRO

MAIS OPÇÕES

0 Software(s)

Exibir: 15

Ordenar por: Avaliação

Nenhum software encontrado. Tente outros filtros

CATÁLOGO DE SOFTWARE PÚBLICO

Resultado da pesquisa

PESQUISAR CATÁLOGO DE SOFTWARE

Todos

Software Público

workload segmentation

FILTRO

MAIS OPÇÕES

0 Software(s)

Exibir: 15

Ordenar por: Avaliação

Nenhum software encontrado. Tente outros filtros

9.7. Análise às políticas, modelos e padrões de governo segundo o artigo 11, alínea C da IN SGD/ME nº 94/2022:

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1	X	X	
	Solução 2		X	
	Solução 3		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

10. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

- 10.1. Diante da necessidade de renovar o ambiente tecnológico da PCDF, no que diz respeito à segurança da informação, e a fim de atender ao objetivo da demanda, foram analisadas as vantagens e desvantagens dos 2 (dois) modelos de soluções identificados, de forma que se conclui pela Solução 1 como tecnicamente viável.
- 10.2. Conforme § 1º do art. 11 na IN 94/2022 SGD/ME, a alternativa 2 foi considerada inviável, portanto, dispensamos a realização dos respectivos cálculos de custo total de propriedade para essa alternativa.

Solução 2 - Gerenciamento Manual via Firewall	
Análise da solução	A alternativa de solução foi afastada devido ao risco de se permanecer com um ambiente crítico, já que o firewall, embora seja uma camada importante de defesa, não é suficiente sozinho para oferecer a profundidade e o nível de controles e visualização necessários. A segmentação oferecida pelo dispositivo não oferece a granularidade necessária para proteger aplicações ou serviços, sendo que todos os dispositivos e sistemas em um mesmo segmento podem se comunicar sem restrições, o que poderia expor a rede de dados a movimentações laterais de ameaças.

10.3. Conforme § 1º do art. 11 na IN 94/2022 SGD/ME, a alternativa 3 também foi considerada inviável, portanto, dispensamos a realização dos respectivos cálculos de custo total de propriedade para essa alternativa.

Solução 3 – Utilização de Solução do portal de Software Público Brasileiro	
Análise da solução	A alternativa de solução foi afastada devido a inexistência de soluções no referido portal que cumpram os requisitos essenciais buscados pela PCDF com esta contratação.

11. ANÁLISE COMPARATIVA DE CUSTOS (TCO – TOTAL COST OF OWNERSHIP)
- 11.1. Cálculo dos Custos Totais de Propriedade e Mapa Comparativo dos Cálculos Totais de Propriedade (TCO):
- 11.1.1. Conforme inciso III do art. 11 da IN SGD/ME nº 94/2022, deve-se proceder à comparação de custos totais de propriedade para as soluções técnica e funcionalmente viáveis.
- 11.1.2. Contudo, diante do fato de que apenas uma solução atende satisfatoriamente o cenário da PCDF, não há viabilidade de realização de análise comparativa de custos e o mapa comparativo final de uma única solução.
- 11.1.3. Por este motivo, será realizado apenas o cálculo dos custos totais de propriedade da única solução tecnicamente viável (Solução 1B) e, por conseguinte, a apresentação do cálculo do custo total da contratação.
12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA
- 12.1. Justificativa do Cenário escolhido
- 12.1.1. A equipe técnica entende que a única solução viável é a Solução 1 – Aquisição de solução de Microsegmentação por promover a evolução tecnológica da infraestrutura de TIC da Instituição, sobretudo no que se refere à proteção dos ativos críticos da PCDF.
- 12.2. Especificações técnicas:
- 12.2.1. Tabela descritiva:
- | ITEM | QTD | DESCRIÇÃO |
|------|------|---|
| 1 | 516 | Solução de Segurança para Microsegmentação de rede - Servidores |
| 2 | 5000 | Solução de Segurança para Microsegmentação de rede - Endpoints |
| 3 | 21 | Solução de Segurança para Microsegmentação de rede - Kubernetes |
| 4 | 1 | Serviço de Instalação da solução |
| 5 | 5 | Serviço de Treinamento/ Capacitação para 5 pessoas |
- 12.3. Descrição técnica detalhada
- 12.3.1. Solução de Segurança para Microsegmentação para ambiente de servidores, estações de trabalho e Kubernetes (Itens 1, 2 e 3)
- 12.3.1.1. Características Gerais
- 12.3.1.1.1. Deverá suportar a microsegmentação tanto em dispositivos físicos quanto em dispositivos virtualizados (independente da tecnologia utilizada para virtualização).
- 12.3.1.1.2. Deverá ser licenciado para todos os servidores, estações de trabalho e kubernetes, objeto da contratação.
- 12.3.1.1.3. Deverá possibilitar a criação de ilhas no ambiente, onde os ativos tenham sua comunicação restrita (tráfego Leste-Oeste/Norte-Sul), apenas ao que for previamente identificado e liberado, principalmente no contexto de aplicações, que devem ter sua comunicação liberada apenas no contexto estritamente necessário.
- 12.3.1.1.4. Toda a solução deverá ser gerenciada por uma console única de gerência centralizada, para todos os tipos de ativos especificados anteriormente. Serão aceitas exceções em casos de integrações com soluções de terceiros, quando especificado;
- 12.3.1.1.5. Toda a solução deverá ser do mesmo fabricante, sem qualquer tipo de customização não autorizada pelo mesmo.
- 12.3.1.1.6. A solução não poderá ser baseada em ferramentas open source.
- 12.3.1.1.7. Deverá ser oferecido retenção mínima de 45 dias para todos os dados enviados para a console, incluindo os fluxos de rede coletados, permitindo através desses fluxos a construção de mapas com retenção de pelo menos 90 dias;
- 12.3.1.1.8. Deverá suportar, minimamente, a instalação de agentes nos seguintes sistemas operacionais:
- 12.3.1.1.8.1. Amazon Linux;
- 12.3.1.1.8.2. CentOS Linux: 5.2 (32 bits), 5.2 até 5.11 (64 bits), 6 até 9 (64 bits);
- 12.3.1.1.8.3. Oracle Linux: 5.2 até 5.11, 6 até 9 (todos 64 bits);
- 12.3.1.1.8.4. Red Hat Linux: 5, 5.1, 5.2 até 5.11, 6, 7 e 8 (todos 64 bits);
- 12.3.1.1.8.5. Debian Linux: 7.5 até 12 (todos 64 bits);
- 12.3.1.1.8.6. Ubuntu Linux: 12.04 até 22.04 LTS (todos 64 bits);
- 12.3.1.1.8.7. Windows Server 2003 SP2 (32 e 64 bits), 2008 (32 bits), 2008 R2, 2012, 2016, 2016 Core, 2019 e 2022;
- 12.3.1.1.8.8. Windows Desktop: 7 (32 e 64 bits), 8 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11;
- 12.3.1.1.8.9. MacOS 11 ou superior.
- 12.3.1.1.9. No caso de dispositivos que não possam receber os agentes, a solução deverá disponibilizar um mecanismo que permita cadastrar os mesmos e criar regras para ditar como estes recursos podem interagir com a rede protegida.
- 12.3.1.1.10. Deverá suportar a segmentação de ambientes em contêineres, atendendo minimamente as seguintes plataformas e tecnologias relacionadas:
- 12.3.1.1.10.1. Orchestration Platforms;
- 12.3.1.1.10.2. AWS Elastic Kubernetes Service (EKS);
- 12.3.1.1.10.3. Azure Kubernetes Service (AKS);
- 12.3.1.1.10.4. Kubernetes;
- 12.3.1.1.10.5. OpenShift;
- 12.3.1.1.10.6. Rancher Kubernetes Engine (RKE);
- 12.3.1.1.10.7. Container Runtime;
- 12.3.1.1.10.8. Containerd;
- 12.3.1.1.10.9. Docker;
- 12.3.1.1.10.10. CRI-O;
- 12.3.1.1.10.11. Network Plugins;
- 12.3.1.1.10.12. Kubelet;
- 12.3.1.1.10.13. Azure CNI;
- 12.3.1.1.10.14. Calico;
- 12.3.1.1.10.15. OVN-Kubernetes (OVN);
- 12.3.1.1.10.16. Canal.
- 12.3.1.1.11. Ser capaz de visualizar todo o fluxo de dados dos PODs no mesmo mapa de fluxo de dados, ou seja, o mapa de fluxo de dados deverá ser único para Servidores, Desktops, Cloud Workload e PODs;

- 12.3.1.1.12. Ser possível configurar regras de controle para comunicações no ambiente. Estas regras deverão também ser baseadas em etiquetas.
- 12.3.1.1.13. Deverá também refletir de forma automática, qualquer alteração de metadados e labels do cluster, ajustando as regras de segmentação já criadas;
- 12.3.1.1.14. Deverá apresentar informações de comunicação entre os PODs, incluindo qual o processo (container) que originou ou recebeu a comunicação, a porta e o protocolo utilizado, além da imagem e linha de comando utilizada, suportando a identificação de uso indevido dentro da plataforma de kubernetes;
- 12.3.1.1.15. Deverá apresentar o fluxo de dados leste-oeste e norte-sul (comunicação de e para a internet);
- 12.3.1.1.16. A solução não deve gerar nenhum tipo de impacto ou atraso na subida de recursos do ambiente de kubernetes (PODs, Serviços e Etc);
- 12.3.1.1.17. Deverá ser independente de hardware, ou seja, funcionar em qualquer infraestrutura de rede composta pela compatibilidade requerida já especificada.
- 12.3.1.1.18. Não deverá ser necessário qualquer parada (downtime) dos servidores ou aplicações, incluindo, mas não se limitando:
- 12.3.1.1.18.1. Reinício (Reboot) dos ativos, sejam servidores, estações de trabalho ou Nodes;
- 12.3.1.1.18.2. Alteração de IPs, Nomes, configurações de rede em geral, dos ativos;
- 12.3.1.1.18.3. Alteração da infraestrutura de rede, seja ela física ou virtual.
- 12.3.1.1.18.4. A solução deverá suportar IPv4 e IPv6;
- 12.3.1.1.19. Deverá ser capaz de monitorar todos os fluxos de tráfego do Datacenter: Leste-Oeste (servidor-servidor) e Norte-Sul (rede cliente-servidor ou servidor-externa, ou seja, internet). Ou seja, a solução deve monitorar os fluxos de tráfego de todos os ativos que possuem agentes instalado, incluindo o fluxo entre máquinas virtuais em execução no mesmo hipervisor, ativos de tipos diferentes, comunicação entre nuvem pública com datacenter privado, entre outros.
- 12.3.1.1.20. A solução também deverá permitir a criação de regras de filtragem de comunicação entre distintos tipos de ativos, bem como entre distintos tipos de ambientes;
- 12.3.1.1.21. A solução deverá manter registro de todos os Fluxos de Ativos, incluindo os que não foram bloqueados bem como aqueles que falharam (ex.: Timeout);
- 12.3.1.1.22. Toda a comunicação interna entre os componentes da solução deve ser completamente criptografada e autenticada;
- 12.3.1.1.23. A solução deverá possuir no mínimo as seguintes certificações de segurança: ISO 27001, ISO 27018 e SSAE 16 Type 2 (SOC2);
- 12.3.1.2. **Arquitetura e implementação**
- 12.3.1.2.1. Não serão aceitas soluções que sejam “Forks” de projetos de software existentes, ou seja, versões derivadas que tenham sido modificadas a partir do código fonte original.
- 12.3.1.2.2. Caso a solução suporte o modelo de serviço de nuvem (SaaS), a mesma deverá estar hospedada em um dos principais fornecedores de nuvem pública como Amazon, Google ou Microsoft, geograficamente localizada em território brasileiro, não sendo permitido sobre qualquer circunstância a transferência dos dados coletados para fora do território brasileiro.
- 12.3.1.2.3. A plataforma SaaS do fornecedor deve possuir certificação SOC 2 Tipo 2 emitido por auditor independente.
- 12.3.1.2.4. Para garantir os dados da PCDF, 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 todos os outros componentes na nuvem do fabricante da solução.
- 12.3.1.2.5. A Console de Gerenciamento deverá ser única e centralizada para toda a Solução.
- 12.3.1.2.6. Os agentes deverão se comunicar diretamente com a plataforma SaaS sem a necessidade de agregadores caracterizando-se assim uma aplicação de duas camadas.
- 12.3.1.2.7. O agente deverá suportar a utilização de servidores proxies caso o seguimento de rede não possua comunicação direta com a internet.
- 12.3.1.2.8. Os componentes administrativos da solução não deverão possuir dependência de nenhum outro componente de rede ou infraestrutura para o seu perfeito funcionamento.
- 12.3.1.2.9. A implementação do agente deverá ser compatível com ferramentas de deployment de software de uso geral como SCCM, Chef, Ansible, Puppet ou outra que seja passível de execução de um script shell ou PowerShell.
- 12.3.1.2.10. A solução deverá utilizar agentes instalados nos ativos protegidos, responsável por coletar fluxos de dados e garantir a aplicabilidade das regras configuradas;
- 12.3.1.2.11. Deverá proporcionar a instalação do agente de forma manual, através de msi e scripts já elaborados e disponibilizados pelo fabricante da solução.
- 12.3.1.2.12. O agente deverá suportar a opção de auto proteção contra remoção, cabendo ao administrador habilitar ou desabilitar esta opção via console de gerenciamento.
- 12.3.1.2.13. O processo de instalação, atualização ou remoção dos agentes da solução não deverá exigir a reinicialização de dispositivos.
- 12.3.1.2.14. Deverá possibilitar a implementação dos agentes em modo apenas de monitoramento, fornecendo visibilidade do tráfego para que o administrador da solução possa criar regras e planejar a mudança para modo bloqueio com visibilidade e contexto de todo o tráfego de rede.
- 12.3.1.2.15. A solução deverá permitir a criação de políticas, fornecendo apenas a visibilidade e impacto das mesmas, para posterior provisionamento da mesma e enforcement das regras.
- 12.3.1.2.16. Deverá permitir integração via SAML 2.0 com IDPs externos, como no mínimo o Microsoft Azure AD\Entra, possibilitando autenticação na console administrativa a partir de um usuário gerenciado internamente pela CONTRATANTE.
- 12.3.1.2.17. Deverá possuir auditoria para rastreamento de todas as modificações realizadas na console administrativa.
- 12.3.1.2.18. Deverá possibilitar a capacidade de filtragem de tráfego com base em aplicações, rótulos, ambientes, período de tempo, status da política, etc. Permitindo ainda exportação dos logs para consumo externo a ferramenta.
- 12.3.1.2.19. Não deverá haver limitação de número de regras e quantidade de tráfego a ser analisado pela ferramenta.
- 12.3.1.2.20. A comunicação entre o agente e a console central deverá ser criptografada.
- 12.3.1.2.21. Deverá possuir capacidade de etiquetamento de todos os ativos, incluindo os que possuem agentes ou outros ativos sem agentes, mas que se comunicaram ou receberam comunicação de um ativo protegido pela solução
- 12.3.1.3. **Características da Console de Gerenciamento**
- 12.3.1.3.1. A console deverá ser única para toda a solução de microssegmentação;
- 12.3.1.3.2. Ter a capacidade de gerenciar todos os tipos de ativos (servidores, cloud, estações de trabalho e Kubernetes) em uma única console;
- 12.3.1.3.3. Ter a capacidade de visualizar os fluxos de dados e configurar as políticas de segurança em uma única console;
- 12.3.1.3.4. Possuir um Dashboard com as principais informações referentes ao ambiente;
- 12.3.1.3.5. Ter a capacidade de visualizar em modo gráfico, através de mapas, os fluxos de dados do ambiente;
- 12.3.1.3.6. Visualizar todos os ativos protegidos, incluindo informações como Nome, Sistema Operacional e IP;
- 12.3.1.3.7. Ter a capacidade de visualizar todas as etiquetas associadas a um único dispositivo;
- 12.3.1.3.8. Ter a capacidade de visualizar todos os ativos para uma única etiqueta;
- 12.3.1.3.9. Deve ser possível filtrar os fluxos de comunicação de dados, no mínimo em:
- 12.3.1.3.9.1. Bloqueado ou Permitido;
- 12.3.1.3.9.2. Origem: por etiqueta e nome do ativo;
- 12.3.1.3.9.3. Destino: por etiqueta e nome do ativo;
- 12.3.1.3.9.4. Comunicações com Origem ou Destino para a Internet;

- 12.3.1.3.9.5. Pelo nome do conjunto de regras de proteção aplicado no ambiente;
- 12.3.1.3.9.6. Porta e Protocolo;
- 12.3.1.3.9.7. Período de tempo;
- 12.3.1.3.9.8. Por processo utilizado da comunicação;
- 12.3.1.3.9.9. Ser possível criar novas etiquetas e gerenciar etiquetas existentes;
- 12.3.1.3.9.10. Exportar as etiquetas, no mínimo em CSV ou XLS;
- 12.3.1.3.9.11. Ter a capacidade, através de interface gráfica na própria console, de monitorar a saúde de todos os componentes da solução, no mínimo para os agentes e Clusters Kubernetes
- 12.3.1.3.9.12. Ter a capacidade, através de interface gráfica na própria console, de parar e reiniciar os componentes da solução, no mínimo para os agentes, coletores e servidores de Relay, ou possuir proteção nativa contra parada dos agentes, reiniciando automaticamente em caso de erro;
- 12.3.1.3.9.13. 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;
- 12.3.1.3.10. Deve possuir Logs de Auditoria, para no mínimo:
 - 12.3.1.3.10.1. Autenticação do usuário: Com sucesso e falha de autenticação;
 - 12.3.1.3.10.2. Política de Segmentação: Criação e alteração de políticas, bem como a ação de desabilitar a política;
 - 12.3.1.3.10.3. Etiquetas: Criação e alteração;
 - 12.3.1.3.10.4. Logs: Quem consultou os logs;
- 12.3.1.3.11. Os Logs de Auditoria devem conter, no mínimo: O dia, hora, Ação Executada, Nome do usuário, IP de Origem e Descrição;
- 12.3.1.3.12. Deve ser possível gerenciar os usuários com acesso a solução, não havendo limites para o número de usuários existentes;
- 12.3.1.3.13. Deve possuir integração com sistemas de diretório para integração de autenticação. Deve ser compatível com mínimo com LDAP e SAML 2.0;
- 12.3.1.3.14. Deve suportar autenticação Kerberos;
- 12.3.1.3.15. Deve ser possível criar usuários locais, e gerenciar os usuários existentes.
- 12.3.1.3.16. Deve suportar segundo fator de autenticação;
- 12.3.1.3.17. Possuir níveis de permissões diferentes para os usuários, no mínimo com as seguintes características:
 - 12.3.1.3.17.1. Administrador da solução;
 - 12.3.1.3.17.2. Somente Leitura;
 - 12.3.1.3.17.3. Somente visualização dos Incidentes;
 - 12.3.1.3.17.4. Administração das Políticas;
- 12.3.1.3.18. Ser possível verificar todos os incidentes gerados pela solução diretamente na própria console de administração;
- 12.3.1.3.19. Deve ser possível customizar o nível de criticidade dos incidentes;
- 12.3.1.3.20. 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;
- 12.3.1.3.21. 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;
- 12.3.2. **Características do Agentes**
 - 12.3.2.1. A solução deverá possuir agentes instalados nos ativos protegidos;
 - 12.3.2.2. Os agentes deverão ser compatíveis com as seguintes plataformas, no mínimo:
 - 12.3.2.2.1. Windows Server 2003 SP2 (32 e 64 bits), 2008 (32 bits), 2008 R2, 2012, 2016, 2016 Core, 2019 e 2022;
 - 12.3.2.2.2. Windows Desktop: 7 (32 e 64 bits), 8 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11;
 - 12.3.2.2.3. MacOS 11 ou superior;
 - 12.3.2.2.4. Red Hat Linux: 5, 5.1, 5.2 até 5.11, 6, 7 e 8 (todos 64 bits);
 - 12.3.2.2.5. CentOS Linux: 5.2 (32 bits), 5.2 até 5.11 (64 bits), 6 até 9 (64 bits);
 - 12.3.2.2.6. Oracle Linux: 5.2 até 5.11, 6 até 9 (todos 64 bits);
 - 12.3.2.2.7. Alma 8 e 9 (64bits);
 - 12.3.2.2.8. Amazon Linux;
 - 12.3.2.2.9. Amazon Linux 2;
 - 12.3.2.2.10. Ubuntu Linux: 12.04 até 22.04 LTS (todos 64 bits);
 - 12.3.2.2.11. Debian Linux: 7.5 até 12 (todos 64 bits);
 - 12.3.2.2.12. SUSE Linux: 11, 12 e 15 (todos 64 bits);
 - 12.3.2.2.13. Solaris: 10.8 até 10.11 (x86_64 e SPARCv9), 11 até 11.4 (x86_64 e SPARCv9);
 - 12.3.2.2.14. AIX: 6.1, 7.1, 7.2 e 7.3;
 - 12.3.2.2.15. Rocky 8 e 9 (64bits);
 - 12.3.2.3. Para Containers e Kubernetes, a solução deverá atuar como um DaemonSet em todos os Nós do Cluster;
 - 12.3.2.4. Deverá coletar todos os fluxos de dados de comunicação entre PODs, bem como origem e/ou destino de infraestrutura não baseada em micro serviço;
 - 12.3.2.5. Os agentes deverão consumir no máximo 5% de CPU;
 - 12.3.2.6. Os agentes deverão ser capazes de coletar informações do ativo, como flows de rede, e executar as políticas de proteção;
 - 12.3.2.7. As políticas de proteção deverão permanecer em execução mesmo que o ativo não tenha acesso a Console de Gerenciamento;
 - 12.3.2.8. Os agentes deverão armazenar os Logs de Fluxo de Dados e Incidentes mesmo que o ativo não tenha acesso a Console de Gerenciamento;
 - 12.3.2.9. Caso os agentes não sejam uma implementação nativa de Firewall e dependam do Firewall do Sistema Operacional, deverão atender os seguintes requerimentos mínimos:
 - 12.3.2.9.1. Deverá estender as capacidades técnicas do Firewall do Sistema Operacional, não se limitando somente a versão nativamente existente, devendo atender aos it técnicos deste documento;
 - 12.3.2.9.2. Deverá possuir controles nativos da solução que evitem alteração nas políticas definidas pelo administrador da solução de microssegmentação;
 - 12.3.2.9.3. Deverá possuir controles nativos que impeçam a parada do Firewall do Sistema Operacional;
 - 12.3.2.9.4. Bloquear caso o administrador da rede, ou do sistema operacional, tente efetuar alterações manuais nas regras de firewall diretamente no próprio Sistema Operacional;

- 12.3.2.9.5. Bloquear caso outra solução, como um Antivírus ou EDR, tente efetuar a parada ou desinstalação do Firewall nativo do sistema operacional;
- 12.3.2.9.6. Bloquear a tentativa de parada, desinstalação ou comprometimento do Firewall nativo do Sistema Operacional em casos de ataques;
- 12.3.2.9.7. O Fabricante da solução de Microsegmentação deverá garantir a atualização, ou mecanismos de contorno/proteção, em caso de conhecidas e/ou publicação de novas vulnerabilidades existente no Firewall nativo do Sistema Operacional;
- 12.3.2.9.8. Deverá suportar o uso do agente da solução em conjunto com o Firewall Nativo do Sistema Operacional, ou de terceiros, exceto em casos de Limitação do Sistema Operacional;
- 12.3.2.10. Os agentes deverão capturar todos os Fluxos de Dados nos ativos instalados e enviar para a console de gerenciamento.
- 12.3.2.11. As informações capturadas pelo agente deverão conter no mínimo:
 - 12.3.2.11.1. IP de Origem e Destino;
 - 12.3.2.11.2. Hostname de Origem e Destino;
 - 12.3.2.11.3. Porta e Protocolo;
 - 12.3.2.11.4. Quantidade de conexões;
 - 12.3.2.11.5. Hora e Data;
 - 12.3.2.11.6. Informações do processo/binário responsável pela comunicação, na origem e destino;
 - 12.3.2.11.7. Caminho do binário no ativo;
 - 12.3.2.11.8. Nome do Serviço do Windows (Ex.: BITS) responsável pela comunicação, quando este for executado em um processo padrão (Ex.: SVCHost.exe);
 - 12.3.2.11.9. Usuário que executou o processo;
 - 12.3.2.11.10. FQDN ou IP, quando for um acesso com origem ou destino para Internet;
- 12.3.2.12. A instalação do agente não deverá requer qualquer tipo de parada no Sistema Operacional, incluindo reiniciar (Reboot);
- 12.3.2.13. A instalação do agente não deverá requerer qualquer tipo alteração no ativo, como mudança de IP, Hostname, ou instalação de software que possam comprometer o funcionamento normal da aplicação;
- 12.3.2.14. Os agentes deverão ter a capacidade de coletar informações dos ativos que estão instalados, como exemplo, mas não se limitando: Processos em execução, uptime do sistema, entre outros;
- 12.3.2.15. **Característica de Visibilidade**
 - 12.3.2.15.1. A solução deverá, a partir da instalação dos agentes, fornecer um mapa de dependência de aplicativos em tempo real de como a comunicação de rede está acontecendo, de forma a proporcionar o completo entendimento dos administradores para uma melhor tomada de decisão.
 - 12.3.2.15.2. Além do mapa visual de comunicações, a solução ainda deverá fornecer meios para filtragem específica de comunicações em modo de log na console, contendo no mínimo os detalhes de origem, destino, portas, protocolos e aplicações internas que realizaram a comunicação.
 - 12.3.2.15.3. Deverá possuir, no mapa de rede, filtros de inclusão e exclusão, permitindo filtrar no mínimo:
 - 12.3.2.15.3.1. IP;
 - 12.3.2.15.3.2. Porta;
 - 12.3.2.15.3.3. Aplicação, Binário e Serviço;
 - 12.3.2.15.3.4. Nome do Ativo;
 - 12.3.2.15.3.5. Tipo de Conexão - Estabelecida, bloqueada e as que violaram uma política;
 - 12.3.2.15.3.6. Internet - Com Origem e Destino da Internet;
 - 12.3.2.15.3.7. Usuário que iniciou o processo;
 - 12.3.2.15.4. A tela do Mapa de Dados deve possuir mecanismo de busca;
 - 12.3.2.15.5. Deve reter os fluxos de dados por um mínimo de 45 dias, sendo possível criar ou visualizar os mapas utilizando períodos históricos;
 - 12.3.2.15.6. O mapa de dados deverá apresentar informações de comunicação em Camada 4 e Camada 7;
 - 12.3.2.15.7. Deverá ser possível verificar as Etiquetas aplicadas a um ativo diretamente da tela do Mapa de Dados;
 - 12.3.2.15.8. Ser possível identificar a quantidade de vezes que uma determinada comunicação aconteceu em um período de tempo;
 - 12.3.2.15.9. Ser possível, no mapa de dados, obter informações do processo que efetuou uma determinada comunicação, possuindo no mínimo informações do Caminho do Binário no Ativo, o usuário que executou o processo e a linha de comando executada;
 - 12.3.2.15.10. Deve ser possível, no mapa de dados, visualizar as comunicações de todos os ativos do ambiente, máquina a máquina;
 - 12.3.2.15.11. Deve ser possível, no mapa de dados, agrupar os ativos através das etiquetas existentes no ambiente, permitindo ainda hierarquizar em subgrupos;
 - 12.3.2.15.12. Deve registrar e apresentar todos os fluxos de comunicação do datacenter, em formato de tabela, juntamente com informações contextuais e detalhadas sobre as cargas de trabalho e aplicativos (processos) de comunicação;
 - 12.3.2.15.13. Deve fornecer recursos de filtragem (Ip/Porta/Processo/Origem/Destino/Usuário que iniciou a comunicação) se a comunicação foi estabelecida/bloqueada;
 - 12.3.2.15.14. Deve descobrir automaticamente qualquer novo fluxo de comunicação em tempo real;
 - 12.3.2.15.15. Deve ser possível filtrar os fluxos de dados por um conjunto de regras aplicados no ambiente;
 - 12.3.2.15.16. Deve ser possível exportar os fluxos de dados no mínimo em CSV;
 - 12.3.2.15.17. Deve ser possível visualizar todos os ativos, através da console, obtendo informações da primeira vez que foi visto e a última vez que o ativo se comunicou com a console;
 - 12.3.2.15.18. Deverá ser possível etiquetar ou aplicar TAGs nos ativos do ambiente, ativos com agentes e sem agentes, para utilizar tanto na visualização, em políticas bem como em filtros;
 - 12.3.2.15.19. A etiquetas deverão seguir um modelo de Categoria e Valores, por exemplo Ambiente / Produção, ou de forma similar onde é possível incluir valores diferentes para uma mesma categoria;
 - 12.3.2.15.20. As etiquetas deverão ser criadas através da própria console de gerenciamento, no mínimo das seguintes formas:
 - 12.3.2.15.20.1. Dinamicamente - Ex: Todo dispositivo que o nome contém PROD, ou que estão na subrede 10.0.0.0/8, aplicar Etiqueta Ambiente: Produção
 - 12.3.2.15.20.2. Através de integração com CMDB - Coletar os dados diretamente da solução de CMDB utilizada;
 - 12.3.2.15.20.3. Através de Integração com sistemas que já possuem TAGs - Como VMWare VCenter, Nuvens públicas (AWS, GCP, Azure, OCI), Kubernetes (Metadados dos clusters) e CSV;
 - 12.3.2.15.20.4. Através de APIs públicas;
 - 12.3.2.15.20.5. Deverá ser possível agrupar etiquetas em Grupos de Etiquetas, para uso nas políticas e outras partes da solução;
 - 12.3.2.15.20.6. Deverá ser registrado em Log toda a criação, remoção ou modificação das etiquetas, informando no mínimo o usuário responsável, hora e data e a etiqueta alterada. Esses logs deverão ser acessíveis através da própria console de gerenciamento;

- 12.3.2.15.20.7. Deverá ser possível aplicar uma etiqueta a um único dispositivo, e também a um conjunto de dispositivos;
- 12.3.2.15.21. A console de gerenciamento deverá possuir uma área específica de informações dos ativos que devem apresentar todas as Etiquetas aplicadas ao ativo;
- 12.3.2.15.22. As etiquetas poderão ser utilizadas no Mapa de Visualizações de Fluxo de Dados e na criação de políticas;
- 12.3.2.15.23. Deverá apresentar no mapa de fluxo de dados os dispositivos gerenciados e não-gerenciados pela solução.
- 12.3.2.15.24. A visão detalhada dos logs deve permitir a criação de regras para fluxos detectados como bloqueados a partir de interação com os logs, apenas selecionando as comunicações desejadas.
- 12.3.2.15.25. A solução deve realizar sugestões inteligentes de como a regra deverá ser criada, de forma a facilitar a ação do administrador da ferramenta.
- 12.3.2.15.26. A visão detalhada do tráfego de rede deverá mostrar quais os processos do sistema operacional foram responsáveis por aquela comunicação, permitindo ainda que as regras possam controlar essa comunicação apenas quando esse mesmo processo iniciar a comunicação, garantindo que aquela comunicação de fato corresponde a aplicação de origem para a plataforma do sistema operacional.
- 12.3.2.15.27. Os agentes da solução deverão alimentar continuamente a console central, de forma que o administrador de rede sempre tenha contexto atualizado sobre as comunicações que estão ocorrendo.
- 12.3.2.15.28. A visibilidade gerada pela solução deverá suportar conceitos de RBAC, ou seja, segmentar a possibilidade de controle e visibilidade na console baseado no nível de permissão atribuído ao administrador autenticado na plataforma.
- 12.3.2.15.29. Os dados de visibilidade deverão estar disponíveis para consulta na console por pelo menos 90 dias.
- 12.3.2.16. **Regras de segmentação e visibilidade**
- 12.3.2.16.1. A solução deverá fornecer a capacidade de criar, gerenciar e monitorar políticas de tráfego Leste-Oeste e Norte-Sul flexíveis até o nível de uma única carga de trabalho e aplicativo (processo ou serviço do MS Windows);
- 12.3.2.16.2. Deve permitir criar e monitorar políticas de comunicação de aplicativo a partir do mapa de visualização;
- 12.3.2.16.3. Deve suportar regras definidas sobre grupos de ativos de acordo com sua função ou etiquetamento;
- 12.3.2.16.4. Deve possuir no mínimo 2 (dois) tipos de regras:
- 12.3.2.16.4.1. Bloqueio; e
- 12.3.2.16.4.2. Permissão.
- 12.3.2.16.5. Deverá permitir a criação de regras de microsegmentação utilizando os seguintes parâmetros:
- 12.3.2.16.5.1. Etiquetas e Grupo de Etiquetas;
- 12.3.2.16.5.2. Ativo (nome do ativo);
- 12.3.2.16.5.3. IP/Subrede;
- 12.3.2.16.5.4. Aplicação / Processo do Windows (Ex.: BITS);
- 12.3.2.16.5.5. Grupo de usuários;
- 12.3.2.16.5.6. FQDN;
- 12.3.2.16.5.7. Internet (Comunicação vindo da Internet / Rede Interna);
- 12.3.2.16.5.8. Qualquer (Any).
- 12.3.2.16.6. Deverá possuir filtros de informações no gerenciamento das regras do ambiente;
- 12.3.2.16.7. Deve salvar as revisões de política e permitir a reversão para versões anteriores;
- 12.3.2.16.8. A solução deverá possuir nativamente modelos (templates) pré-definidos para aplicações conhecidas de mercado (Ex.: Active Directory), tendo o catálogo disponibilizado na própria console de gerenciamento;
- 12.3.2.16.9. Deverá possuir nativamente modelos (templates) pré-definidos para políticas de Prevenção de Ransomware;
- 12.3.2.16.10. Deverá sugerir a criação de regras de forma automática com base no fluxo histórico de comunicação das aplicações
- 12.3.2.16.11. Deve poder sugerir políticas automaticamente de acordo com os dados coletados;
- 12.3.2.16.12. A solução deverá possuir mecanismos que através dos fluxos de dados históricos, possam sugerir a criação de regras de acesso.
- 12.3.2.16.13. Deve ser possível criar políticas com Lógicas de E e OU;
- 12.3.2.16.14. A solução deverá permitir a inclusão de listas de FQDNs, através de importação de arquivo, para serem utilizadas durante a consulta DNS em bloqueio ou liberação de acesso a sites específicos;
- 12.3.2.16.15. Deve permitir a criação de regras com usuários em ambientes VDI/Terminal/Citrix de forma a garantir que apenas determinados grupos do Active Directory possam chegar a determinados endereços e/ou aplicações na rede;
- 12.3.2.16.16. Deverá fornecer dados e contexto para detecção de tentativas de movimento lateral
- 12.3.2.16.17. Deve registrar tentativas de violação da política e fornecer informações detalhadas sobre a violação da conexão, indicando inclusive qual processo iniciou a comunicação;
- 12.3.2.16.18. A solução deverá permitir a criação de etiquetas a serem aplicadas nas cargas de trabalho, de maneira que a identificação dos servidores e aplicações do ambiente sejam facilmente reconhecidos.
- 12.3.2.16.19. As etiquetas deverão suportar o conceito de escopo da rede, ou seja, produção, homologação e desenvolvimento, assim como a qual ambiente e localização o ativo está incluso.
- 12.3.2.16.20. As regras deverão ser criadas baseadas em dois critérios principais, sendo eles: Escopo interno, ou seja, apenas entre serviços pertencentes a mesma aplicação identificada ou também no contexto de escopo externo, no caso de aplicações diferentes que precisam de comunicação de rede entre si.
- 12.3.2.16.21. Todas as etiquetas e atributos definidos nos tópicos anteriores deverão estar disponíveis amplamente para criação de políticas, seja pelo papel que o ativo executa, ou aplicação representada, ambiente ou localização.
- 12.3.2.16.22. As regras deverão possibilitar a criação granular, baseado nas etiquetas e atributos solicitados, baseados em origem, destino, porta, protocolo, aplicação e processos do sistema operacional
- 12.3.2.16.23. As regras deverão conseguir utilizar listas de IPs, sub redes, FQDNs, range de portas e portas customizadas para controles específicos.
- 12.3.2.16.24. Deverá suportar a utilização de portas dinâmicas, ou seja, baseado no processo do sistema operacional e não em um range específico.
- 12.3.2.16.25. A solução deverá permitir a duplicação de políticas por parte do administrador, de forma a facilitar o processo de criação de regras.
- 12.3.2.16.26. A solução deverá suportar a importação e exportação de políticas.
- 12.3.2.16.27. A solução deverá permitir a atribuição de políticas em grupos específicos de hosts ou em hosts específicos.
- 12.3.2.16.28. No caso de remoção do agente da solução, todas as regras criadas deverão ser imediatamente removidas.
- 12.3.2.16.29. A solução deverá possuir integração nativa com scanners de vulnerabilidade para controle contextual de ativos com base nas vulnerabilidades que ele possui.
- 12.3.2.16.30. Essa integração deverá permitir a ingestão de dados de, pelo menos, os seguintes fabricantes: Qualys e Tenable.
- 12.3.2.16.31. A solução deverá permitir integração com Active Directory para controle de regras de acesso baseado em grupos do Active Directory.
- 12.3.2.16.32. A solução deverá suportar meios para visualização de impacto das políticas antes de aplicação de modificações das mesmas.

- 12.3.2.16.33. A visibilidade da solução deverá permitir facilmente a identificação de quais tráfegos estão ocorrendo por qual política definida e até mesmo se não existe uma política para o tráfego identificado.
- 12.3.2.16.34. O enforcement de políticas e instalação do agente não deverá requerer nenhum tipo de modificação no kernel do sistema operacional.
- 12.3.2.16.35. A solução deverá suportar o controle de políticas para regras de inbound e outbound no firewall dos ativos protegidos.
- 12.3.2.16.36. Deverá ser possível a criação de regras para “isolamento” de ativos na rede, de forma que a comunicação dos mesmos seja restrita apenas ao que tenha sido previamente definido, impedindo, por exemplo, que ativos contaminados por ameaças possam se comunicar na rede com os demais servidores do datacenter.
- 12.3.2.16.37. Deverá possibilitar a integração com recursos IPSEC nativos do sistema operacional para criptografar o tráfego entre componentes protegidos pela solução.
- 12.3.2.16.38. As políticas da solução deverão possibilitar a coexistência com políticas de firewall que já existam em determinados hosts protegidos
- 12.3.2.16.39. Deverá permitir a identificação e proteção do ambiente a partir de componentes que não tenham o agente instalado.
- 12.3.2.16.40. O agente da solução deverá se automonitorar quanto a falhas de processo ou eventos de adulteração e reiniciar, se necessário, para garantir a funcionalidade contínua.
- 12.3.2.16.41. O agente da solução deverá monitorar continuamente as regras aplicadas evitando assim que as mesmas sejam modificadas ou mesmo eliminadas (“anti tampering”).
- 12.3.2.16.42. O agente deverá ser protegido por uma senha adicional prevenindo a remoção acidental ou proposital do mesmo.
- 12.3.2.16.43. Deverá reter ao menos as 100 versões da política para rollback em caso de necessidade e remoção automática das versões mais antigas para melhorar o desempenho.
- 12.3.2.17. **Gestão de vulnerabilidades**
- 12.3.2.17.1. A solução deverá possuir integração nativa com scanners de vulnerabilidade para realizar o controle contextual de ativos com base nas vulnerabilidades identificadas nos mesmos.
- 12.3.2.17.2. Essa integração deverá permitir a ingestão de dados de, pelo menos, os seguintes fabricantes: Qualys e Tenable.
- 12.3.2.17.3. A solução deverá gerar visões específicas, a partir da ingestão de dados de vulnerabilidades, sobre como as portas e aplicações vulneráveis estão se comunicando na rede corporativa.
- 12.3.2.17.4. Deverá permitir, a partir da integração com scanners de vulnerabilidade, a coleta de metadados e a criação de etiquetas baseadas nas vulnerabilidades existentes
- 12.3.2.17.5. Quando não existir a possibilidade de correção da vulnerabilidade do ativo, a solução deverá fornecer sugestões de ajustes para regras de micros segmentação daquele ativo, de forma a mitigar o maior número possível de brechas do mesmo.
- 12.3.2.18. **API e integrações**
- 12.3.2.18.1. A solução deverá possuir uma API forte e bem documentada.
- 12.3.2.18.2. Via API deverá ser possível realizar operações em políticas e controlar os ativos da solução.
- 12.3.2.18.3. Deverá ser baseada em HTTP e ser compatível com métodos GET, PUT, POST e DELETE.
- 12.3.2.18.4. Deverá ser autenticada via chave a ser gerada no portal da solução.
- 12.3.2.18.5. Deverá possibilitar integração com ferramentas DevOps como Chef, Puppet, Ansible e SCCM.
- 12.3.2.18.6. Deverá possuir integração com ferramentas de SIEM, sendo no mínimo suportado as soluções QRadar, Splunk, Arcsight ou ElasticSearch.
- 12.3.2.18.7. Deverá possuir integração com ferramentas de análise de vulnerabilidades, para coleta de metadados e posterior criação de etiquetas baseadas nas vulnerabilidades existentes;
- 12.3.2.18.8. Deverá possuir integração com F5 BIG-IP;
- 12.3.2.18.9. Deverá possuir integração com Firewall Fortigate da Fortinet, ou permitir o uso de API, para envio de IPs maliciosos;
- 12.3.2.18.10. Deverá fornecer contexto de comunicação em tempo real contendo todas as informações de comunicação de rede;
- 12.3.2.18.11. Deverá permitir envio de relatórios por e-mail;
- 12.3.2.18.12. Deverá permitir a exportação de IOCs.
- 12.3.3. **Requisitos do Serviço de Instalação, implementação e suporte da solução de Microsegmentação de rede (Para os itens 1, 2 e 3)**
- 12.3.3.1. Os serviços de instalação, configuração e documentação deverão ser executados pela equipe técnica da CONTRATADA;
- 12.3.3.2. O(s) profissional(is) técnico(s) da CONTRATADA responsável(is) pela execução dos serviços contratados deve(m) obrigatoriamente possuir os certificados do fabricante da solução.
- 12.3.3.3. **A implantação da solução deverá contemplar as seguintes fases:**
- 12.3.3.3.1. Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas envolvidas, a estratégia de implantação do serviço, o plano de testes, arquitetura da solução, bem como quaisquer outros itens que sejam necessários para a implantação do projeto.
- 12.3.3.3.2. Documentação: deverá ser entregue a documentação do projeto, conforme descrita a seguir, em formato, quantidade e datas a serem acordados entre as partes.
- 12.3.3.3.3. Plano de Requisitos de Infraestrutura: A CONTRATADA deverá, antes do início da execução das configurações, elaborar documentação técnica fundamentando todas as ações que serão realizadas.
- 12.3.3.3.4. Após a aprovação do planejamento pela CONTRATANTE, o processo de implantação será iniciado, levando-se em consideração o cumprimento dos prazos pactuados.
- 12.3.3.3.5. O suporte do desenvolvedor da solução deverá ser 24 horas, 7 dias por semana, 365 dias por ano durante toda a vigência do Contrato.
- 12.3.3.4. **O suporte técnico do fabricante deverá obedecer aos seguintes prazos:**
- 12.3.3.4.1. Severidade **CRÍTICA**: nível aplicado quando há comprometimento imediato do funcionamento da solução (indisponibilidade) CONTRATANTE;
- 12.3.3.4.1.1. **Prazo de início de atendimento**: Até 01 (uma) horas.
- 12.3.3.4.1.2. **Prazo limite de resolução**: Até 24 (vinte e quatro) horas após abertura do chamado remoto.
- 12.3.3.4.1.3. **Sanção em caso de não resolução no prazo determinado**: Glosa de 2% do valor do contrato, por ocorrência, em caso de descumprimento.
- 12.3.3.4.2. Severidade **ALTA**: nível aplicado quando a funcionalidade principal é afetada ou ocorre degradação significativa do desempenho;
- 12.3.3.4.2.1. **Prazo de início de atendimento**: Até 04 (quatro) horas.
- 12.3.3.4.2.2. **Prazo limite de resolução**: Até 72 (setenta e duas) horas após abertura do chamado remoto.
- 12.3.3.4.2.3. **Sanção em caso de não resolução no prazo determinado**: Glosa de 1,5% do valor do contrato, por ocorrência, em caso de descumprimento.
- 12.3.3.4.3. Severidade **NORMAL**: nível aplicado quando há perda parcial ou intermitente de funcionalidades não críticas da solução, sem comprometimento imediato do seu funcionamento
- 12.3.3.4.3.1. **Prazo de início de atendimento**: Até 08 (oito) horas.
- 12.3.3.4.3.2. **Prazo limite de resolução**: Até 8 (oito) dias após abertura do chamado remoto.
- 12.3.3.4.3.3. **Sanção em caso de não resolução no prazo determinado**: Glosa de 0,5% do valor do contrato, por ocorrência, em caso de descumprimento.

- 12.3.3.4.4. Severidade **BAIXA**: nível aplicado quando há solicitação de esclarecimentos técnicos relativos às ocorrências, ao uso e ao aprimoramento dos serviços ofertados;
- 12.3.3.4.4.1. **Prazo de início de atendimento**: Até 24 (vinte e quatro) horas.
- 12.3.3.4.4.2. **Prazo limite de resolução**: Até 10 (dez) dias após abertura do chamado remoto.
- 12.3.3.4.4.3. **Sanção em caso de não resolução no prazo determinado**: Glosa de 0,25% do valor do contrato, por ocorrência, em caso de descumprimento.
- 12.3.3.4.5. O fabricante deverá possuir, falando em língua portuguesa, um responsável dedicado por atuar em ações decorrentes durante o período do contrato, sendo um Facilitador de comunicação entre os times do fabricante, como o suporte por exemplo, e o time da CONTRATANTE. Também será responsável por realizar reuniões trimestrais de acompanhamento da evolução e uso da solução.

- 12.3.4. **Requisitos de Treinamento da Solução de Microsegmentação de Rede**
- 12.3.4.1. Conforme subitem 7.5 deste documento

13. **ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO**

- 13.1. A metodologia utilizada para a composição dos preços e obtenção do preço de referência fundamentou-se nos arts. 99 a 104 do Decreto Distrital nº 44.330/2023, cujo detalhamento da pesquisa e dos cálculos constam na Estimativa de Custo e Orçamento 14 (188091105) e **Memória de Cálculo (SEI)**, artefatos integrantes do processo de planejamento da contratação.
- 13.2. Com base nos valores obtidos, o preço de referência para Contratação de empresa para fornecimento de Solução de Segurança para Microsegmentação de rede, incluindo instalação, implantação, treinamento, garantia técnica, por 12 (doze) meses perfaz o total de **R\$ 4.739.591,71 (quatro milhões, setecentos e trinta e nove mil, quinhentos e noventa e um reais e setenta e um centavos)**, conforme demonstrado na tabela a seguir:

Planilha Comparativa de Preços

Item	Objeto	U.M.	Qtde	Propostas	Valor Unitário (12 meses)	Valor Mediano Unitário das Propostas Válidas	Variação	Valor Unitário Médio (12 meses)	Valor Unitário Mediano (12 meses)	Valor Unitário Mínimo (entre média e mediana)	Valor Total Estimado
1	Fornecimento de Solução de segurança para microsegmentação de ambiente corporativo com licenciamento para Servidores	Licenças	516	Empresa 1	R\$ 2.988,73	R\$ 3.362,12	-11%	R\$ 3.261,11	R\$ 3.175,42	R\$ 3.175,42	R\$ 1.638.
				Empresa 2	R\$ 5.881,49		75%				
				Empresa 3	R\$ 2.514,83		-25%				
				Empresa 4	R\$ 3.362,12		0%				
							24%				
	PRODEB - PE 001/2025 (item 1)	R\$ 4.178,76									
2	Fornecimento de Solução de microsegmentação de ambiente corporativo com licenciamento para Endpoints	Licenças	5000	Empresa 1	R\$ 404,57	R\$ 494,35	-18%	R\$ 527,95	R\$ 494,35	R\$ 494,35	R\$ 2.471.
				Empresa 2	R\$ 718,52		45%				
				Empresa 3	R\$ 519,67		5%				
							-5%				
				Empresa 4	R\$ 469,04						
3	Fornecimento de Solução de microsegmentação de ambiente corporativo com licenciamento para Kubernetes.	Licenças	21	Empresa 1	R\$ 13.781,59	R\$ 13.781,59	0%	R\$ 13.862,58	R\$ 13.781,59	R\$ 13.781,59	R\$ 289.4
				Empresa 2	R\$ 22.041,96		60%				
				Empresa 3	R\$ 2.514,83		-82%				
				Empresa 4	R\$ 14.025,00		2%				
							0%				
	PRODEB - PE 001/2025 (item 2)	R\$ 13.781,16									
4	Serviço de Instalação da solução	Serviço	1	Empresa 1	R\$ 200.000,00	R\$ 220.000,00	-9%	R\$ 225.868,30	R\$ 220.000,00	R\$ 220.000,00	R\$ 220.0
				Empresa 2	R\$ 220.000,00		0%				
				Empresa 3	R\$ 22.888,75		-90%				
				Empresa 4	R\$ 662.694,48		201%				
					R\$ 257.604,90		17%				
5	Serviço de Treinamento/ Capacitação para 5 pessoas	Serviço	5	Empresa 1	R\$ 28.886,40	R\$ 28.886,40	0%	R\$ 26.384,78	R\$ 23.982,32	R\$ 23.982,32	R\$ 119.9
				Empresa 2	R\$ 41.700,00		44%				
				Empresa 3	R\$ 15.874,50		-45%				
				Empresa 4	R\$ 92.226,93		219%				
					R\$ 19.078,25		-34%				
VALOR DE REFERÊNCIA TOTAL DA CONTRATAÇÃO											R\$ 4.739.

14. **JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO**

- 14.1. A equipe técnica após estudo dos cenários acima descritos, entende que a Solução 1B – **Aquisição de Solução de Microsegmentação** se apresenta como a melhor solução por proporcionar aumento significativo da proteção do ambiente de rede de dados contra ataques do tipo ransomware, movimentações laterais, minimização de risco de ataques internos, visibilidade e controle detalhado sobre o tráfego de rede facilitando a identificação de possíveis incidentes de segurança, além de facilitar a auditoria nesses casos.

15. **DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS E ECONÔMICOS**

- 15.1. Para que todos os serviços sejam prestados pela CONTRATADA – que irá fornecer a solução de Segurança as licenças de software e serviços correlatos (implementação e treinamento) – a CONTRATANTE solicita que a licitação ocorra em grupo único. Tratam-se de itens distintos de uma única solução, separados em itens por questões de clareza na composição e formação dos custos. Dissociar serviços e produtos de um único fornecimento traz prejuízos ao conjunto por razões de aumento da complexidade do gerenciamento, conflito de interesse entre diferentes partes prestadoras, além da privação dos ganhos de escala trazidos pela contratação em lote único.
- 15.2. O agrupamento dos diferentes itens da solução em grupo único não implica em restrição de competitividade, uma vez que os fornecedores dos serviços do mercado estão aptos a atender todos os itens especificados no grupo, mesmo que, caso necessário, seja feita a composição de diferentes ferramentas. Logo, além de ser um imperativo técnico, não há qualquer impedimento ou restrição do ponto de vista do mercado de fornecedores para que os itens venham a ser prestados por uma única empresa.
- 15.3. Do ponto de vista da eficiência técnica, a contratação em um único grupo é mais vantajosa, pois permite a plena integração entre os componentes da solução

de microssegmentação, garantindo visibilidade centralizada dos ativos de rede e controle granular de acessos, bem como a aplicação automatizada de políticas de segmentação de tráfego. A integração entre os módulos da solução viabiliza o mapeamento detalhado das dependências entre aplicações e fluxos de dados, além da resposta automatizada a incidentes de segurança, como tentativas de movimentação lateral e ataques de ransomware.

15.4. Por se tratar de uma solução composta por múltiplos serviços interdependentes — como licenciamento para servidores, endpoints e clusters Kubernetes, implantação técnica, suporte contínuo e capacitação da equipe — a contratação conjunta se mostra fundamental para assegurar a qualidade das entregas e o desempenho adequado da solução como um todo. Isso otimiza recursos, facilita a gestão contratual em um único ponto e reduz o tempo de resposta em caso de falhas, contribuindo diretamente para a continuidade operacional e o aumento da resiliência cibernética da instituição.

15.5. Não há prejuízo à ampla competitividade, uma vez que existem diversos fornecedores no mercado capazes de ofertar a solução de forma integrada, conforme as especificações técnicas e regulatórias exigidas.

15.6. Conforme deliberações do TCU sobre a matéria, como a decisão que afirma que “**A aquisição de itens diversos em lotes deve estar respaldada em critérios justificantes**”, adotando o entendimento do Acórdão nº 5260/2011, de 06/07/2011, que decidiu que “**Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si**”.

15.7. Fundamenta-se ainda na necessidade de integração entre os componentes geridos por uma única empresa contratada, reduzindo o tempo de resposta caso ocorram problemas e proporcionando maior efetividade e entrega de informações integradas que consolidem os resultados dos diversos componentes implantados.

15.8. Resta claro que o agrupamento dos itens em lote único não é opcional, mas sim, rigorosamente necessário para uma manutenção efetiva das licenças de software e serviços exclusivos ao software adquirido, não cabendo, assim, dividir o fornecimento do objeto em lotes distintos.

16. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

16.1. Tem por objetivo o registro dos benefícios econômicos da solução escolhida em relação às demais soluções analisadas, devendo-se levar em conta não apenas o menor custo do item, mas todos os demais custos levantados no TCO.

16.2. Uma vez que se identificou apenas uma solução considerada viável, não sendo possível a comparação dos cálculos totais de propriedade dentre as soluções consideradas viáveis, deixa-se de se apresentar a justificativa econômica da escolha da solução.

17. 4. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

17.1. Complementar significativamente as estratégias de segurança multicamada da Instituição, dificultando a concretização de acessos indevidos (redução da superfície de ataque);

17.2. Contribuir para a garantia da disponibilidade e continuidade dos serviços de Tecnologia da Informação;

17.3. Agilidade na reação às ameaças e ataques, a partir da detecção de vulnerabilidades de segurança em tempo real, reduzindo o tempo de resposta;

17.4. Possibilidade de tratar e auditar ações em caso de incidentes de segurança, proporcionando subsídios para tomada de decisões e melhorias dos processos falhos;

17.5. Correlacionamento de eventos de segurança, permitindo a criação de inteligência de ameaças, a partir da identificação de padrões de comportamento que possam indicar uma anomalia ou ataque;

17.6. Resiliência Cibernética, aumentando a proteção do ambiente contra ataques avançados, como ransomware, de movimentação lateral ou ataques direcionados (APT- Advanced Persistent Threat), restringindo a propagação de ameaças dentro da rede;

17.7. Microssegmentação da rede, com configurações de comunicação entre as partes estritamente necessárias, de acordo com as políticas previamente estabelecidas, mitigando os riscos de segurança.

17.8. Mapeamento da rede corporativa permitindo correção de vulnerabilidades entre as comunicações internas;

17.9. Garantia de meios seguros para acesso remoto ao ambiente;

17.10. Automação de políticas de segurança, garantindo que as políticas sejam aplicadas consistentemente, independentemente da localização física dos recursos;

17.11. Isolamento granular de sistemas sensíveis, a partir da ação que permite dividir a rede em segmentos menores, isolando sistemas críticos, como bancos de dados de inteligência e dados corporativos de outros sistemas menos críticos;

17.12. Limitação de acesso dos usuários internos a sistemas e dados estritamente relevantes para suas funções, prevenindo abusos de acesso ou espionagem interna;

17.13. Visibilidade sobre interações entre sistemas e usuários na rede, facilitando o monitoramento contínuo do tráfego pela equipe de segurança.

17.14. Flexibilidade e escalabilidade permitindo ajustes, na medida em que a PCDF adquira novos sistemas e dispositivos integrando-os à estrutura existente.

17.15. Facilitação da gestão de políticas de segurança em ambientes híbridos, garantindo que a segurança seja mantida de forma consistente, independentemente da localização dos sistemas ou dos dados.

17.16. Automatização de respostas a ameaças detectadas, como o isolamento de um segmento comprometido, acelerando a contenção dos incidentes.

17.17. Redução de custos com incidentes de segurança uma vez que a prevenção de ataques e a minimização de danos causados por invasores, ajuda a reduzir significativamente os custos associados à recuperação de incidentes de segurança;

17.18. Continuidade Operacional no momento em que isolando incidentes, ajuda a garantir a continuidade dos serviços da PCDF, minimizando o impacto das interrupções, evitando que um ataque tome grandes proporções e paralise a entrega dos serviços essenciais à população.

18. PROVIDÊNCIAS A SEREM ADOTADAS

18.1. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL

18.1.1. **Recursos materiais:** Adequação não é necessária.

18.1.2. **Recursos tecnológicos:** Servidores de rede para instalação da solução.

18.1.3. **Recursos humanos:** Adequação não é necessária.

18.1.4. **Espaço Físico/Mobiliário:** Adequação não é necessária.

18.2. NECESSIDADES DE CAPACITAÇÃO DE SERVIDORES PARA GESTÃO E FISCALIZAÇÃO CONTRATUAL

18.2.1. Não há a necessidade de capacitação específica de servidores para gestão e fiscalização contratual.

18.3. AÇÕES PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

18.3.1. Na presente contratação não há indicação de ações destinadas à transição e encerramento contratual a serem feitas.

18.4. CONTRATAÇÃO CORRELATA E/OU INTERDEPENDENTE

18.4.1. Não se verificam contratações correlatas ou interdependentes que sejam necessárias para a viabilidade e execução desta demanda.

18.5. ALINHAMENTO AO PLANO ANUAL DE COMPRAS E CONTRATAÇÕES PACC

18.5.1. O objeto da contratação encontra-se alinhado ao item 34 Anexo B do caderno explicativo de investimentos do Plano Anual de Compras e Contratações da PCDF para o ano de 2025.

19. CLASSIFICAÇÃO DO ETP

19.1. A equipe de planejamento da contratação deve proceder à classificação do ETP, em estrita observância ao artigo 65 do Decreto Distrital nº 44.330/2023 a seguir transcrito:

Art. 65. Ao final da elaboração do ETP, deve-se avaliar a necessidade de classificá-lo nos termos da Lei nº 12.527, de 18 de novembro de 2011, da Lei nº 4.990, de 12 de dezembro de 2012, e do Decreto nº 34.276, de 11 de abril de 2013, que regulam o acesso a informações.

19.2. Em atenção ao art. 65 do Decreto nº 44.330/2023, após avaliação, a equipe de planejamento da contratação constatou que não há necessidade de classificação deste ETP, por não haverem informações que se enquadrem no rol das informações que devem ser classificadas, nos termos da [Lei nº 12.527, de 18 de novembro de 2011](#), da

20. DECLARAÇÃO DE VIABILIDADE

20.1. O presente planejamento foi elaborado em harmonia com a IN SGD/ME nº 94, de 23 dezembro de 2022 e em consonância ao Decreto nº 44.330 de 16 de março de 2023, que regulamenta a Lei nº 14.133/2021, de 1º de abril de 2021, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios. À luz do art. 269-A do referido Decreto, que determina a adoção da regulamentação editada pela União sobre as contratações de bens e serviços de tecnologia da informação, utilizou-se a Instrução Normativa SGD/ME nº 94/2022 e normativos correlatos para fundamentar e nortear o planejamento das contratações de soluções TIC na PCDF.

20.2. O presente planejamento está de acordo com as necessidades técnicas, operacionais e estratégicas do órgão. Encontra-se também em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição. No mais, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomendamos a contratação proposta.

20.3. Em conformidade com o art. 11, da IN SGD/ME nº 94, de 23 dezembro de 2022, e em observância à fundamentação descrita no início deste documento, este Estudo Técnico Preliminar demonstra a viabilidade técnica e econômica para a contratação em tela nos moldes definidos neste documento.

Integrante Requisitante: Carlos Said Oiticica Bandeira, Matrícula nº 78.156-8

Integrante Técnico: Tulio Andre Pereira De Oliveira, Matrícula nº 1.716.240-8

21. RESPONSÁVEIS

21.1. A Equipe de Planejamento da Contratação foi instituída por meio de Despacho do Senhor Diretor do Departamento de Administração Geral - DAG (SEI 149265337), em 22/08/2024.

INTEGRANTE TÉCNICO: Tulio Andre Pereira De Oliveira, Matrícula nº 1.716.240-8

INTEGRANTE REQUISITANTE: Carlos Said Oiticica Bandeira, Matrícula nº 78.156-8

22. APROVAÇÃO DA AUTORIDADE COMPETENTE

22.1. Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

Simone Pereira Duarte Ferreira

Matrícula nº 078.526-1

Diretora da DITEC/DGI/PCDF



Documento assinado eletronicamente por **TÚLIO ANDRÉ PEREIRA DE OLIVEIRA - Matr.1716240-8, Agente de Polícia Civil**, em 05/12/2025, às 16:28, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



Documento assinado eletronicamente por **SIMONE PEREIRA DUARTE FERREIRA - Matr.0078526-1, Diretor(a) da Divisão de Tecnologia**, em 09/12/2025, às 17:14, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



Documento assinado eletronicamente por **CARLOS SAID OITICICA BANDEIRA - Matr.0078156-8, Chefe do Serviço de Segurança em Tecnologia da Informação**, em 19/12/2025, às 14:22, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



A autenticidade do documento pode ser conferida no site:
[http://sei.df.gov.br/sei/controlador_externo.php?](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
[acao=documento_conferir&id_orgao_acesso_externo=0](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
verificador= 175070351 código CRC= 8ED0728A.

"Brasília - Patrimônio Cultural da Humanidade"

SPO, Lote 23, Conjunto A, Bloco H, Centro Tecnológico, Térreo - Bairro Setor Policial - CEP 70610-907 - DF

Telefone(s): (61) 3207-5147

Sítio - www.pcdf.df.gov.br