MINISTÉRIO DA ECONOMIA
Secretaria Especial de Desburocratização, Gestão e Governo Digital
Secretaria de Governo Digital
Departamento de Plataformas

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo nº 19974.100786/2022-07

AQUISIÇÃO CENTRALIZADA DE SOLUÇÃO DE CRIPTOGRAFIA DE LINKS DE COMUNICAÇÃO DE DADOS

0.0.1.

HISTÓRICO - REVISÕES			
Data	**Versão**	**Descrição**	
19/05/2022	1.0	Criação do Documento	
	1.1	Revisão e Ajustes	
	2.0	Revisão e Ajustes após IRP	
	2.1	Revisão e ajustes após interações com o mercado e órgão de controle	
	2.2	Revisão e ajustes após análise da PGFN	

1. INTRODUÇÃO

1.1. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda (SEI-ME n° 24189586), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o processo de contratação, em consonância com o art. 11 da Instrução Normativa SGD-ME nº 01/2019.

1.2. O objeto do estudo é a **aquisição de solução de criptografia de links de comunicação via internet com vista a promover a confidencialidade das informações trafegadas, com estrutura redundante, alta capacidade de tráfego e elevado nível de segurança, incluindo serviços de instalação, implantação e suporte técnico, para atender os órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP**.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1. **Identificação das necessidades de negócio**

2.1.1. As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (Guia BABOK v. 2.0), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição daquela considerada mais adequadas a tais objetivos organizacionais.

2.1.2. A Secretaria de Governo Digital (SGD), da Secretaria Especial de Desburocratização, Gestão e Governo Digital (SEDGG), do Ministério da Economia tem a missão de "Transformar o governo pelo digital, promovendo a efetividade das políticas, a qualidade dos serviços e reconquistando a confiança dos brasileiros". Para atender esse foco estratégico, é preciso que os órgãos do governo federal sejam capazes de comunicarem-se de forma segura e ininterrupta.

2.1.3. Atualmente a maior parte dos dados críticos que circulam entre os órgãos do governo é feita por meio de links de internet dedicados fornecidos por diversas operadoras do mercado (Oi, Embratel, Claro, Vivo, Telefônica etc.). São inúmeros links dedicados contratados de forma independente por cada órgão federal, além da própria Infovia Brasília, que é gerida pelo Ministério da Economia e operada pelo Serviço Federal de Processamento de Dado (Serpro).

2.1.4. A infraestrutura dos links de dados dos órgãos do governo federal requer mais atenção à medida que novas aquisições ou atualizações de seus componentes tornam o ambiente mais complexo. Assim, é preciso conhecer e tratar eventuais falhas de segurança na forma de um processo contínuo, visando antecipar riscos e agir de forma proativa. Sabe-se que a grande malha de links existentes e o alto volume de dados críticos trafegados nessa rede tornam o governo federal alvo de ataques cibernéticos de toda natureza.

2.1.5. Apesar da grande preocupação de todo o governo federal e dos altos investimentos que tem sido realizados na disciplina de cibersegurança e segurança da informação, na maioria das situações não se tem dado a devida atenção na proteção do links de comunicação de dados.

2.1.6. Uma solução de criptografia de links é um dos pilares da iniciativa de segurança e proteção de dados para se estabelecer para o governo federal. Trata-se de uma solução complementar às demais soluções vinculadas à área de segurança. De forma didática, pode-se elencar três pilares de soluções estratégicas com vista a estabelecer um ambiente adequado à proteção de dados críticos no governo federal e ampliar a aderência a normativos relacionados à segurança e proteção de dados:

- 1º Pilar: proteções perimetrais (segurança de rede/borda);
- 2º Pilar: criptografia e anonimização de dados (segurança na base de dados); e
- 3º Pilar: criptografia de links de internet (segurança na comunicação).

2.1.7. A criptografia de links é um método de proteção necessário para garantir a devida segurança na transmissão de dados entre os diversos órgãos públicos que se utilizam de links dedicados de internet, da Infovia Brasília ou de outras redes metropolitanas. Com esse método, todo o canal de transmissão (ponta a ponta) é protegido. Tal solução tem foco na proteção do túnel e não do dado propriamente dito. São utilizados equipamentos e softwares específicos para essa finalidade, além de dispositivos especializados que dificultam a localização do tráfego. Quando o link de comunicação é criptografado, entende-se que toda a transmissão de dados se torna segura e deixa de ser vulnerável em caso de interceptação ou ataque cibernético.

2.1.8. Como já mencionado, uma solução de criptografia de links é um pilar adicional que complementa outras soluções já adquiridas ou em estudo pelos órgãos do governo federal no que tange à segurança da informação. Nota-se que a maior parte dos investimentos realizados são direcionados para ferramentas chamadas “perimetrais” (barreiras de acesso) e ativos de segurança para a proteção contra acessos externos mal-intencionados. Tais investimentos concentram-se em ferramentas tipicamente associadas a proteções da rede externa. Todavia, tendo em vista a evolução da sofisticação dos ataques cibernéticos, faz-se necessário o complemento da segurança, traduzida sob a forma da presente demanda.

2.1.9. Resultados da Contratação (resultados negociais)

- Mitigar os riscos de incidentes de segurança envolvendo vazamento e exposição de dados trafegados nas redes do Governo Federal.
- Estabelecer ações preventivas com relação a possíveis ataques cibernéticos.
- Atingir conformidade com a Lei 13.709 – Lei Geral de Proteção de Dados e demais padrões de segurança recomendados para órgãos da administração pública no que concerne a proteção de dados.
- Atuar em respeito ao preceito constitucional para a proteção do direito fundamental de proteção de dados pessoais dos cidadãos que se relacionam com os órgãos públicos federais e demais pessoas sob a égide da Constituição Federal.
- Proteção de dados sensíveis que trafegam nas redes de comunicação de dados do governo federal;
- Atuação preventiva com relação a vazamento de dados;
- Criar um ambiente de rede WAN protegido, contra interceptação indevida do tráfego de dados;

2.2. **Identificação das necessidades tecnológicas**

2.2.1. No entendimento da equipe de planejamento da contratação a criptografia de link fim-a -fim tem uma grande relevância porque abrange a segurança do ambiente computacional e a garantia de alta disponibilidade dos recursos tecnológicos que são necessários para manter níveis de serviços adequados para o correto funcionamento do ambiente de infraestrutura.

2.2.2. Com o intuito de prover os órgãos do SISP de uma solução que auxilie a criação e manutenção de um processo contínuo de proteção de dados. Sem um processo que proteja o dado, seja onde ele estiver, a Administração Pública estará sujeita a passar por incidentes de segurança com grave impacto ao desempenho institucional dos órgãos, tais como indisponibilidade nos serviços fornecidos, acesso e distribuição ilegal de informações e tempo investido pela equipe no tratamento e resposta de ocorrências.

2.2.3. As necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, descrevem as características de uma solução que atenda aos requisitos do negócio. São desenvolvidos e definidos neste documento os seguintes requisitos tecnológicos:

a) Proteção a partir da camada 2 do modelo OSI**:** No que diz respeito aos links de operadoras, que implementam circuitos virtuais, compartilhados entre seus diversos clientes é necessário garantir a segurança dos dados do governo federal que trafegam nestes circuitos. A implementação de criptografia fim-a-fim com segurança das chaves criptográficas é o único método de proteção neste caso;

b) Criptoagilidade: Também conhecida como agilidade criptográfica, trata-se de um paradigma de prática no projeto de protocolos e padrões de segurança da informação de forma que possam suportar vários algoritmos criptográficos ao mesmo tempo. Um sistema de segurança é considerado cripto ágil se seus algoritmos criptográficos ou parâmetros podem ser substituídos com facilidade e é pelo menos parcialmente automatizado. A criptoagilidade permite redução de TCO, permitindo que equipamentos com essa funcionalidade possam ser atualizados com novos algoritmos de mercado e até mesmo customizados, sem que seja necessária a troca dos equipamentos.

c) Conformidade com padrões internacionais de segurança padrão como FIPS 140-2 Level 3, NATO E Common Criteria EAL2+;

d) Baseado em appliance dedicado para a função de criptografia garantindo a independência dos equipamentos de Firewall e Roteadores. A implementação de técnicas de criptografia consome recursos de processamento. Desta forma se tal funcionalidade fosse aplicada por firewalls e ou roteadores, esses equipamentos precisariam de dimensionamento específico aumentando o TCO para equipamentos que não são especializados na operação de criptografia; e

2.3. **Demais requisitos necessários e suficientes à escolha da solução de TIC**

2.3.1. Além dos requisitos de negócio e tecnológicos, a presente seção destaca aqueles requisitos que devem ser considerados ao longo do planejamento da contratação para se assegurar o alcance dos objetivos pretendidos com a aquisição, conforme a seguir:

Tabela 1 - Requisitos complementares

REQUISITOS	JUSTIFICATIVA
Suportar requisitos da LGPD	Buscando apoiar nas iniciativas de conformidade com a lei geral de proteção de dados.
Requisitos Sociais, Ambientais e Culturais	Deverá fornecer as licenças de software de forma eletrônica, evitando a confecção e transporte de mídias.
Requisitos de implementação	Deverá ser elaborado conjuntamente com o projeto de implementação da solução.
Requisitos de transferência de conhecimento	Deverá ser elaborado um material e disponibilizado para a equipe de fiscalização contratual.
Requisitos de suporte técnico	Os produtos que compõem a solução não devem estar com término de comercialização (*End-of-Sale*) anunciado, isto é, devem estar em produção e serem comercializados pelo fabricante no momento da assinatura do Pedido de Compra / Contrato. Após ser anunciado o término da comercialização (*End-of-Sale*) dos produtos que o compõem a solução, o suporte (*End-of-Support*) deverá permanecer por, no mínimo, o período de vigência da garantia.
Requisitos de suporte técnico	As empresas fornecedoras da solução deve ter representação no Brasil
Requisitos de qualidade	Os equipamentos que constituem a solução a ser fornecida deverão ser novos e com versão de *software* atualizada, não sendo aceitos equipamentos remanufaturados

3. DESCRIÇÃO DA SOLUÇÃO TECNOLÓGICA

3.1. A solução ofertada deve reduzir ao máximo a ocorrência de incidentes internos de segurança através de criptografia de links;

3.2. A solução ofertada deve estabelecer um modelo de proteção para informações de tal forma que o dado seja devidamente criptografado a partir da camada 2 do modelo OSI.

3.3. A Solução ofertada deve permitir topologias ponto-a-ponto, ponto-multiponto e full-mesh;

3.4. A solução ofertada deve ser flexível e escalável, adequando-se às necessidades de crescimento da empresa contratante;

3.5. A Solução ofertada deve implementar mecanismos de proteção contra acesso físico com certificação FIPS ou equivalente.

3.6. A solução ofertada deve ser administrada por console de gerenciamento centralizada, com gestão de chaves criptográficas baseada em hardware para facilitar o processo de administração, controle de acesso, gestão, logs e manutenção.

3.7. ***Appliance* de criptografia de links tipo1**

Características de Hardware

3.7.1. O equipamento deve permitir ser montado em rack padrão de 19” (dezenove polegadas), sendo fornecido com todos os acessórios indispensáveis para sua instalação e funcionamento.

3.7.2. Deve possuir altura máxima de 1 (uma) unidade de rack (1RU).

3.7.3. O equipamento deve suportar no mínimo 2 (duas) fontes de energia internas, para Corrente Alternada (AC – Alternating Current), com chaveamento automático e capacidade de operação em 100V à 240V (50/60Hz), conforme abaixo:

3.7.3.1. As fontes de energia devem permitir utilização de circuitos elétricos distintos;

3.7.3.2. As fontes de energia devem ser do tipo substituível (hot-swap), permitindo instalação e substituição sem a necessidade de remoção do equipamento;

3.7.3.3. As fontes de energia devem ser suficientes para manter todas as operações do equipamento, mesmo no caso de falha de uma das fontes de energia, independentemente da quantidade de interfaces em uso ou funcionalidades habilitadas;

3.7.3.4. As fontes de energia devem vir acompanhadas com cabos de energia com 1,80m (hum metro e oitenta centímetros) de comprimento mínimo e tomada padrão NBR 14136;

3.7.3.5. Os sistemas de fonte de alimentação devem ser o de maior capacidade oferecido pelo fabricante para o equipamento.

3.7.4. Deve possuir memória não-volátil com capacidade suficiente para armazenar, no mínimo, uma nova versão de sistema operacional que tenha o tamanho de 3 (três) vezes o sistema operacional na versão mais recente, atendendo simultaneamente a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.

3.7.5. Deve possuir configuração de CPU e memória RAM suficiente para a implementação de todas as funcionalidades descritas nesta especificação.

3.7.6. Caso o fabricante possua mais de uma versão de uma mesma placa para atendimento a esta especificação, deve ser fornecida a versão mais recente.

3.7.7. O produto deverá permanecer em linha de produção durante 5 anos após a assinatura do contrato, ou seja, a proponente deve comprovar o seu roadmap neste período.

3.7.8. Deverá possuir módulos de ventilação redundantes e hot-swappable;

3.7.9. "Possuir ventilação ""front-to-back"", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento, sendo permitida também a saída de ventilação lateral.

3.7.10. Deve possuir bateria no próprio appliance com capacidade de backup de suprimento de todas as chaves de cifragem e parâmetros.

3.7.10.1. A bateria deve ter uma vida útil de pelo menos sessenta meses; e

3.7.10.2. O equipamento deve ser capaz de alertar quando a bateria deve ser substituída.

3.7.11. Deve operar em temperaturas ambiente entre 0°C e 40ºC;

3.7.12. Deve ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 0 % a 80% (sem condensação);

3.7.13. Deve suportar temperatura ambiente de armazenamento entre -25ºC e 70ºC;

3.7.14. O sistema operacional / firmware dos equipamentos fornecidos deve, dentro das características solicitadas, ser a versão mais recente no momento da instalação.

3.7.15. Deverá possuir e suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento.

3.7.16. O equipamento deverá permitir a colocação e retirada dos módulos de forma “hot-swap", caso o equipamento seja modular.

3.7.17. O equipamento deverá possuir as interfaces localizadas na parte frontal.

3.7.18. O equipamento deve implementar, no momento da entrega, todas as características exigidas nesta especificação sem a necessidade de inclusão de nenhum componente, módulo ou dispositivo extras.

3.7.19. Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9 ou uma porta de console com interface USB.

3.7.19.1. Deve ser fornecido cabo de console compatível com a porta de console do equipamento.

3.7.20. Deve prover mecanismos de proteção e tentativas de acesso indevido ao interior do hardware.

3.7.21. Caso haja uma tentativa indevida de acesso ao interior do hardware, o próprio equipamento deverá apagar todas as configurações e chaves armazenadas nele.

3.7.22. O equipamento deve possuir trava mecânica e módulo de segurança embutido.

3.7.23. O equipamento deve ter a capacidade de demonstrar evidências de adulteração.

Gerenciamento

3.7.24. A solução deve suportar e estar licenciada para gerenciar todos os módulos de criptografia envolvidos neste fornecimento.

3.7.25. Deve permitir que todos os módulos de criptografia sejam controlados de forma centralizada, utilizando apenas um servidor de gerência, mesmo que módulo criptográfico e o servidor de gerência estejam em sub-redes diferentes.

3.7.26. A solução de gerenciamento deve permitir ser replicada nos Data Center da CONTRATANTE, fornecendo redundância entre cada um.

3.7.27. Todos os softwares de gerência necessários para o controle dos módulos de criptografia devem ser fornecidos pela CONTRATADA.

3.7.28. A solução de gerenciamento deve ser capaz de configurar todas as funcionalidades dos módulos de criptografia, sem a necessidade de acesso pela porta console dos appliances para fazer configurações adicionais.

3.7.29. Deve permitir a gerência através de interface WEB ou de software cliente, desde que todos os softwares necessários sejam fornecidos.

3.7.30. Caso o software de gerência deva ser instalado em *appliances* ou outro equipamento específico dedicado, a contratada deverá fornecê-lo com o devido hardware.

3.7.31. O software do servidor de gerência deve, dentro das características solicitadas, ser a versão atual mais estável no momento da instalação.

3.7.32. As mensagens de gerenciamento criptografadas podem ser transferidas para as unidades de criptografia on-line e off-line.

3.7.33. Deve incluir um canal de comunicação seguro, com criptografia baseada em certificados, entre os servidores de gerência e todos os módulos de criptografia distribuídos que fazem parte de um único domínio de gerenciamento da solução.

3.7.34. A solução de gerência deve incluir uma interface gráfica que forneça uma maneira simples de monitorar os *appliances*, exibindo inclusive os estados dos LEDs dos *appliances*.

3.7.35. Um sistema de backup/restore de todas as configurações da solução de gerência deve estar incluso e deve permitir ao administrador agendar backups da configuração em um determinado dia e hora.

3.7.36. Caso os *appliances* percam comunicação com o servidor de gerência, o tráfego entre os módulos de criptografia não pode ser interrompido.

3.7.37. Os logs gerados pelos *appliances* devem ser centralizados no servidor de gerência.

3.7.38. Os logs devem ser transferidos de maneira segura entre os *appliances* e o servidor de gerência ou o servidor dedicado de log, e desses servidores até a interface de visualização de logs na estação do administrador.

3.7.39. A solução deve ser capaz de exportar logs para arquivos externos em formato CSV ou XLS.

3.7.40. Devem ser fornecidos manuais de instalação, configuração e operação da solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade.

3.7.41. Alterações dos endereços IP dos servidores de gerenciamento não deverão causar interrupção de tráfego.

3.7.42. Deverá suportar simultaneamente os padrões de endereçamento IPv4 e IPv6 (RFC 2460).

3.7.43. Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou RFC 2819.

3.7.44. Deve suportar o protocolo de gerenciamento SNMP e MIB-II, em conformidade com os padrões RFCs 1157 e RFC 1213.

3.7.45. Deve suportar os protocolos SNMPv2c e SNMPv3, incluindo a geração de traps.

3.7.46. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:

3.7.46.1. Sem autenticação e sem privacidade (no AuthNoPriv);

3.7.46.2. Com autenticação e sem privacidade (authNoPriv);

3.7.46.3. Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES.

3.7.47. Suportar SNMP sobre IPv6.

3.7.48. Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento.

3.7.49. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.

3.7.50. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.

3.7.51. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.

3.7.52. Deve permitir ser configurável via CLI (Command Line Interface), através de Telnet e SSH, suportando no mínimo, 10 sessões simultâneas e independentes.

3.7.53. Deve permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Túneis IPSEC.

3.7.54. O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, TELNET, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento.

3.7.55. Deve permitir a configuração de endereços IPv6 para gerenciamento.

3.7.56. Deve proteger a interface de gerência do equipamento através de senha.

Interfaces

3.7.57. O equipamento deve ser entregue com no mínimo 1 (uma) interface de 1 Gigabit Ethernet dedicada para o tráfego de gerência.

3.7.58. O equipamento deve ser entregue com no mínimo 4 (quatro) interfaces 10 Gigabit Ethernet no padrão 10GBASE-SR4 (multi mode) ou 10GBASE-LR4 (Single mode) e seus respectivos transceptores.

3.7.59. Alternativamente aos transceivers poderão ser ofertados cabos DAC(Direct Attach Cables) para agregação das portas de 10Gigabit;

3.7.60. Devem ser fornecidos todos os cabos, de até 50 metros, conectores ópticos e transceptores necessários para todas as interfaces e portas do equipamento, sendo que comprimento adequado de cada cabo e os tipos de conectores para fibra serão especificados pela contratante no momento do pedido de compra.

3.7.61. Todas as interfaces devem ser internas ao equipamento, não serão aceitos conversores externos para nenhum tipo de interfaces exigidas.

3.7.62. Deve disponibilizar as facilidades de hot-swap para todos os módulos de interfaces e transceptores.

3.7.63. Deve permitir a reinicialização de interfaces do equipamento sem afetar o funcionamento do mesmo.

3.7.64. Deve permitir a reinicialização de módulos do equipamento sem afetar o funcionamento do mesmo.

3.7.65. Deve possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento.

3.7.66. Deve possuir LEDs de diagnósticos que forneçam informações e atividades das portas.

3.7.67. Para facilitar o manuseio de cabos e conexões, todas as interfaces e portas devem estar localizadas no painel frontal do equipamento.

3.7.68. Os cabos deverão ser fornecidos já conectorizados e deverão ser testados e certificados conforme especificação do fabricante. O certificado poderá ser emitido pelo fabricante, fornecedor do cabo ou pela contratada.

3.7.69. Os transceptores deverão suportar a funcionalidade de hot-swap, sem influenciar o funcionamento do equipamento.

3.7.70. O serviço Ethernet deve executar todas as funções de transporte de todas as aplicações multimídia e deve ser capaz de prover: E-LAN, ELine e E-Tree.

Funcionalidades, Desempenho e Escalabilidade

3.7.71. Deve possuir backplane com throughput mínimo de 10 Gbps (dez gigabit por segundo), considerando 10 Gbps em ambos os sentidos (full-duplex) e pacotes de 600 bytes.

3.7.72. A latência inserida no tráfego de dados deve ser inferior a 10 microssegundos por *appliance*.

3.7.73. Utilizando pacotes com tamanho médio de 600 bytes, o overhead inserido com a criptografia do tráfego deve ser inferior a 5% do tráfego não criptografado.

3.7.74. Deve suportar uma taxa de comutação de pacotes de no mínimo 10 Mpps (dez milhões de pacotes por segundo), considerando-se pacotes de 64 bytes.

3.7.75. Deverá operar em modo ponto-a-ponto, ponto-multiponto e multiponto-multiponto.

3.7.76. O sistema operacional / firmware dos *appliances* fornecidos deve, dentro das características solicitadas, ser a versão atual mais estável no momento da instalação.

3.7.77. O equipamento deve fornecer acesso a uma CLI (interface de linha de comando), sendo acessada localmente via porta de console.

3.7.78. Deve suportar os padrões abertos de gerência de rede SNMPv1, SNMPv2c e SNMPv3, incluindo a geração de traps SNMP para falhas de hardware e eventos, como alterações na configuração do equipamento, por exemplo.

3.7.79. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e interfaces.

3.7.80. Possuir suporte a MIB II, conforme RFC 1213.

3.7.81. Todos os componentes e processos críticos devem gerar logs e permitir gravação dos logs em servidor remoto, através do protocolo syslog.

3.7.82. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

3.7.83. Deve incluir a habilidade de reiniciar o *appliance* para as configurações de fábrica. Esta necessidade deve ser atendida diretamente no painel visual do *appliance*, sem a necessidade de acessá-lo via porta console.

3.7.84. Alterações dos endereços IP dos módulos de criptografia não deverão causar interrupção de tráfego.

3.7.85. Para as operações em rede óptica ou elétricas de alta velocidade a operação deve ser full duplex com garantia de criptografia e descriptografia simultâneas.

Criptografia

3.7.86. A solução de criptografia deve trabalhar em camada 2, criptografando tráfego Ethernet e não necessitando alterar o esquema de roteamento da rede.

3.7.87. Deverá suportar criptografia em camadas 3 e 4 do modelo OSI;

3.7.88. Deve manter as informações de cabeçalho Ethernet e informações de VLAN.

3.7.89. Permitir que o administrador escolha as VLANs cujo tráfego será criptografado, enquanto tráfego relacionados às outras VLANs seja encaminhado sem criptografia.

3.7.90. A criptografia deve ser ultra-segura baseada em hardware com algoritmo secreto específico.

3.7.91. Possibilitar a utilização de algoritmo AES-256, com modos de operação de cifra de bloco GCM ou CTR, para criptografia do tráfego.

3.7.92. Para operações de autenticação e de acordo de chave de sessão, deve permitir a utilização de algoritmos dos sistemas de criptografia de chave pública RSA ou ECC.

3.7.93. Para os algoritmos do sistema de criptografia ECC, deve permitir a utilização de chaves de, no mínimo, 384 bits.

3.7.94. Para os algoritmos do sistema de criptografia ECC, deve permitir a utilização de curvas Brainpool (RFC 5639).

3.7.95. Deve permitir a utilização, sem troca dos equipamentos, de algoritmos personalizados ou curvas elipticas personalizadas;

3.7.96. Para os algoritmos do sistema de criptografia RSA, deve permitir a utilização de chaves de, no mínimo, 2048 bits.

3.7.97. Para geração de hash, deve permitir a utilização do algoritmo SHA-256 ou variações superiores da família SHA-2.

3.7.98. Deve criptografar normalmente tráfego composto de quadros de 9000 bytes (jumboframe), sem realizar qualquer tipo de fragmentação do quadro.

3.7.99. Deve possibilitar a utilização de protocolos de roteamento que utilizam tráfego multicast, podendo esse tipo de tráfego ser encaminhado sem criptografia, se necessário.

3.7.100. O módulo de criptografia deverá preservar o cabeçalho Ethernet dos frames, assim mantendo os endereços MAC de origem e destino, além da identificação da VLAN associada a um determinado frame.

3.7.101. O processo de negociação de chaves de sessão entre os módulos de criptografia deverá ocorrer obrigatoriamente pelas interfaces destinadas para o fluxo de dados de produção, ou seja, não poderá ser feito pelas interfaces de gerência do equipamento.

3.7.102. O administrador deverá poder configurar o tempo de renegociação das chaves de sessão entre os módulos de criptografia, de modo que cada rekey possa ser realizado num período de tempo entre dez e sessenta minutos.

3.7.103. O equipamento deve possuir capacidade de instalação plug-and-play.

Licenciamento

3.7.104. Deve ser licenciado para um número de usuários e endereços IP ilimitados.

3.7.105. Quaisquer licenças necessárias para o funcionamento de todos os recursos e requisitos especificados nesse documento devem ser incluídas e não devem expirar após o término do tempo de vida de suporte dos equipamentos.

Certificações

3.7.106. O produto deve atender aos requisitos de segurança para módulos criptográficos definidos pelo padrão FIPS 140-2 Level 3, NATO E Common Criteria EAL2+

Segurança

3.7.107. O fabricante deve atestar e garantir formalmente que a solução não é passível de sofrer, por qualquer mecanismo ou método: acesso não autorizado, interceptação e monitoramento de comunicações de dados, por força de requerimentos legais ou regulatórios definidos por governos, agências, entidades ou pessoas.

3.8. ***Appliance* de criptografia de links tipo 2**

Características de Hardware

3.8.1. O equipamento deve permitir ser montado em rack padrão de 19” (dezenove polegadas), sendo fornecido com todos os acessórios indispensáveis para sua instalação e funcionamento.

3.8.2. Deve possuir altura máxima de 1 (uma) unidade racks (1RU).

3.8.3. O equipamento deve suportar no mínimo 2 (duas) fontes de energia internas, para Corrente Alternada (AC – Alternating Current), com chaveamento automático e capacidade de operação em 100V à 240V (50/60Hz), conforme abaixo:

3.8.3.1. As fontes de energia devem permitir utilização de circuitos elétricos distintos;

3.8.3.2. As fontes de energia devem ser do tipo substituível (hot-swap), permitindo instalação e substituição sem a necessidade de remoção do equipamento;

3.8.3.3. As fontes de energia devem ser suficientes para manter todas as operações do equipamento, mesmo no caso de falha de uma das fontes de energia, independentemente da quantidade de interfaces em uso ou funcionalidades habilitadas;

3.8.3.4. As fontes de energia devem vir acompanhadas com cabos de energia com 1,80m (hum metro e oitenta centímetros) de comprimento mínimo e tomada padrão NBR 14136;

3.8.3.5. Os sistemas de fonte de alimentação devem ser o de maior capacidade oferecido pelo fabricante para o equipamento.

3.8.4. Deve possuir memória não-volátil com capacidade suficiente para armazenar, no mínimo, uma nova versão de sistema operacional que tenha o tamanho de 3 (três) vezes o sistema operacional na versão mais recente, atendendo simultaneamente a todas as funcionalidades exigidas nesta Especificação, em conformidade com as recomendações do Fabricante.

3.8.5. Deve possuir configuração de CPU e memória RAM suficiente para a implementação de todas as funcionalidades descritas nesta especificação.

3.8.6. Caso o fabricante possua mais de uma versão de uma mesma placa para atendimento a esta especificação, deve ser fornecida a versão mais recente.

3.8.7. O produto deverá permanecer em linha de produção durante 5 anos após a assinatura do contrato, ou seja, a proponente deve comprovar o seu roadmap neste período.

3.8.8. Deverá possuir módulos de ventilação redundantes e hot-swappable;

3.8.9. "Possuir ventilação ""front-to-back"", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento, sendo permitida também a saída de ventilação lateral.

3.8.10. Deve possuir bateria no próprio *appliances* com capacidade de backup de suprimento de todas as chaves de cifragem e parâmetros.

3.8.10.1. A bateria deve ter uma vida útil de pelo menos sessenta meses;

3.8.10.2. O equipamento deve ser capaz de alertar quando a bateria deve ser substituída.

3.8.11. Deve operar em temperaturas ambiente entre 0°C e 40ºC;

3.8.12. Deve ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 0% a 80% (sem condensação);

3.8.13. Deve suportar temperatura ambiente de armazenamento entre -25ºC e 70ºC;

3.8.14. O sistema operacional / firmware dos equipamentos fornecidos deve, dentro das características solicitadas, ser a versão mais recente no momento da instalação.

3.8.15. Deverá possuir e suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento.

3.8.16. O equipamento deverá permitir a colocação e retirada dos módulos de forma “hot-swap", caso o equipamento seja modular.

3.8.17. O equipamento deverá possuir as interfaces localizadas na parte frontal.

3.8.18. O equipamento deve implementar, no momento da entrega, todas as características exigidas nesta Especificação sem a necessidade de inclusão de nenhum componente, módulo ou dispositivo extras.

3.8.19. Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9 ou uma porta de console com interface USB.

3.8.19.1. Deve ser fornecido cabo de console compatível com a porta de console do equipamento.

3.8.20. Deve prover mecanismos de proteção e tentativas de acesso indevido ao interior do hardware.

3.8.21. Caso haja uma tentativa indevida de acesso ao interior do hardware, o próprio equipamento deverá apagar todas as configurações e chaves armazenadas nele.

3.8.22. O equipamento deve possuir trava mecânica e módulo de segurança embutido.

3.8.23. O equipamento deve ter a capacidade de demonstrar evidências de adulteração.

Gerenciamento

3.8.24. A solução deve suportar e estar licenciada para gerenciar todos os módulos de criptografia envolvidos neste fornecimento.

3.8.25. Deve permitir que todos os módulos de criptografia sejam controlados de forma centralizada, utilizando apenas um servidor de gerência, mesmo que módulo criptográfico e o servidor de gerência estejam em sub-redes diferentes.

3.8.26. A solução de gerenciamento deve ter a capacidade de ser fornecendo redundância.

3.8.27. Todos os softwares de gerência necessários para o controle dos módulos de criptografia devem ser fornecidos pela Contratada.

3.8.28. A solução de gerenciamento deve ser capaz de configurar todas as funcionalidades dos módulos de criptografia, sem a necessidade de acesso pela porta console dos *appliances* para fazer configurações adicionais.

3.8.29. Deve permitir a gerência através de interface WEB ou de software cliente, desde que todos os softwares necessários sejam fornecidos.

3.8.30. Caso o software de gerência deva ser instalado em *appliances* ou outro equipamento específico dedicado, a Contratada deverá fornecê-lo com o devido hardware.

3.8.31. O software do servidor de gerência deve, dentro das características solicitadas, ser a versão atual mais estável no momento da instalação.

3.8.32. As mensagens de gerenciamento criptografadas podem ser transferidas para as unidades de criptografia on-line e off-line.

3.8.33. Deve incluir um canal de comunicação seguro, com criptografia baseada em certificados, entre os servidores de gerência e todos os módulos de criptografia distribuídos que fazem parte de um único domínio de gerenciamento da solução.

3.8.34. A solução de gerência deve incluir uma interface gráfica que forneça uma maneira simples de monitorar os *appliances*, exibindo inclusive os estados dos LEDs dos *appliances*.

3.8.35. Um sistema de backup/restore de todas as configurações da solução de gerência deve estar incluso e deve permitir ao administrador agendar backups da configuração em um determinado dia e hora.

3.8.36. Caso os *appliances* percam comunicação com o servidor de gerência, o tráfego entre os módulos de criptografia não pode ser interrompido.

3.8.37. Os logs gerados pelos *appliances* devem ser centralizados no servidor de gerência.

3.8.38. Os logs devem ser transferidos de maneira segura entre os *appliances* e o servidor de gerência ou o servidor dedicado de log, e desses servidores até a interface de visualização de logs na estação do administrador.

3.8.39. A solução deve ser capaz de exportar logs para arquivos externos em formato CSV ou XLS.

3.8.40. Devem ser fornecidos manuais de instalação, configuração e operação da solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade.

3.8.41. Alterações dos endereços IP dos servidores de gerenciamento não deverão causar interrupção de tráfego.

3.8.42. Deverá suportar simultaneamente os padrões de endereçamento IPv4 e IPv6 (RFC 2460).

3.8.43. Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou RFC 2819.

3.8.44. Deve suportar o protocolo de gerenciamento SNMP e MIB-II, em conformidade com os padrões RFCs 1157 e RFC 1213.

3.8.45. Deve suportar os protocolos SNMPv2c e SNMPv3, incluindo a geração de traps.

3.8.46. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:

3.8.46.1. Sem autenticação e sem privacidade (no AuthNoPriv);

3.8.46.2. Com autenticação e sem privacidade (authNoPriv);

3.8.46.3. Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES.

3.8.47. Suportar SNMP sobre IPv6.

3.8.48. Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento.

3.8.49. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa.

3.8.50. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.

3.8.51. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.

3.8.52. Deve permitir ser configurável via CLI (Command Line Interface), através de Telnet e SSH, suportando no mínimo, 10 sessões simultâneas e independentes.

3.8.53. Deve permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Túneis IPSEC.

3.8.54. O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, TELNET, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento.

3.8.55. Deve permitir a configuração de endereços IPv6 para gerenciamento.

3.8.56. Deve proteger a interface de gerência do equipamento através de senha.

Interfaces

3.8.57. O equipamento deve ser entregue com no mínimo 1 (uma) interface de 1 Gigabit Ethernet no padrão 1000BASE-T dedicada para o tráfego de gerência..

3.8.58. O equipamento deve ser entregue com no mínimo 1 (uma) interface 1 Gigabit Ethernet no padrão 10GBASE-SFP+ ou 10GBASE XFP e seus respectivos transceptores.

3.8.59. Devem ser fornecidos todos os cabos, de até 50 metros, conectores ópticos e transceptores necessários para todas as interfaces e portas do equipamento, sendo que comprimento adequado de cada cabo e os tipos de conectores para fibra serão especificados pela Contratante no momento do pedido de compra.

3.8.60. Todas as interfaces devem ser internas ao equipamento, não serão aceitos conversores externos para nenhum tipo de interfaces exigidas.

3.8.61. Deve disponibilizar as facilidades de hot-swap para todos os módulos de interfaces e transceptores.

3.8.62. Deve permitir a reinicialização de interfaces do equipamento sem afetar o funcionamento do mesmo.

3.8.63. Deve permitir a reinicialização de módulos do equipamento sem afetar o funcionamento do mesmo.

3.8.64. Deve possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento.

3.8.65. Deve possuir LEDs de diagnósticos que forneçam informações e atividades das portas.

3.8.66. Para facilitar o manuseio de cabos e conexões, todas as interfaces e portas devem estar localizadas no painel frontal do equipamento.

3.8.67. Os cabos deverão ser fornecidos já conectorizados e deverão ser testados e certificados conforme especificação do fabricante. O certificado poderá ser emitido pelo fabricante, fornecedor do cabo ou pela contratada.

3.8.68. Os transceptores deverão suportar a funcionalidade de hot-swap, sem influenciar o funcionamento do equipamento.

3.8.69. O serviço Ethernet deve executar todas as funções de transporte de todas as aplicações multimídia e deve ser capaz de prover: E-LAN, ELine e E-Tree.

Funcionalidades, desempenho e escalabilidade

3.8.70. Deve possuir backplane com throughput mínimo de 1Gbps (um gigabit por segundo), considerando 1Gbps (um gigabit por segundo em ambos os sentidos ,full-duplex) e pacotes de 600 bytes.

3.8.71. A latência inserida no tráfego de dados deve ser inferior a 10 microssegundos por *appliance*.

3.8.72. Utilizando pacotes com tamanho médio de 600 bytes, o overhead inserido com a criptografia do tráfego deve ser inferior a 5% do tráfego não criptografado.

3.8.73. Deve suportar uma taxa de comutação de pacotes de no mínimo 10 Mpps (dez milhões de pacotes por segundo), considerando-se pacotes de 64 bytes.

3.8.74. Deverá operar em modo ponto-a-ponto, ponto-multiponto e multiponto-multiponto.

3.8.75. O sistema operacional / firmware dos *appliances* fornecidos deve, dentro das características solicitadas, ser a versão atual mais estável no momento da instalação.

3.8.76. O equipamento deve fornecer acesso a uma CLI (interface de linha de comando), sendo acessada localmente via porta de console.

3.8.77. Deve suportar os padrões abertos de gerência de rede SNMPv1, SNMPv2c e SNMPv3, incluindo a geração de traps SNMP para falhas de hardware e eventos, como alterações na configuração do equipamento, por exemplo.

3.8.78. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e interfaces.

3.8.79. Possuir suporte a MIB II, conforme RFC 1213.

3.8.80. Todos os componentes e processos críticos devem gerar logs e permitir gravação dos logs em servidor remoto, através do protocolo syslog.

3.8.81. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

3.8.82. Deve incluir a habilidade de reiniciar o *appliance* para as configurações de fábrica. Esta necessidade deve ser atendida diretamente no painel visual do *appliance*, sem a necessidade de acessá-lo via porta console.

3.8.83. Alterações dos endereços IP dos módulos de criptografia não deverão causar interrupção de tráfego.

3.8.84. Para as operações em rede óptica ou elétricas de alta velocidade a operação deve ser full duplex com garantia de criptografia e descriptografia simultâneas.

Criptografia

3.8.85. A solução de criptografia deve trabalhar em camada 2, criptografando tráfego Ethernet e não necessitando alterar o esquema de roteamento da rede.

3.8.86. Deverá suportar criptografia em camadas 3 e 4 do modelo OSI;

3.8.87. Deve manter as informações de cabeçalho Ethernet e informações de VLAN.

3.8.88. Permitir que o administrador escolha as VLANs cujo tráfego será criptografado, enquanto tráfego relacionados às outras VLANs seja encaminhado sem criptografia.

3.8.89. A criptografia deve ser ultra-segura baseada em hardware com algoritmo secreto específico.

3.8.90. Possibilitar a utilização de algoritmo AES-256, com modos de operação de cifra de bloco GCM ou CTR, para criptografia do tráfego.

3.8.91. Para operações de autenticação e de acordo de chave de sessão, deve permitir a utilização de algoritmos dos sistemas de criptografia de chave pública RSA ou ECC.

3.8.92. Para os algoritmos do sistema de criptografia ECC, deve permitir a utilização de chaves de, no mínimo, 384 bits.

3.8.93. Para os algoritmos do sistema de criptografia ECC, deve permitir a utilização de curvas Brainpool (RFC 5639).

3.8.94. Deve permitir a utilização, sem troca dos equipamentos, de algoritmos personalizados ou curvas elipticas personalizadas;

3.8.95. Para os algoritmos do sistema de criptografia RSA, deve permitir a utilização de chaves de, no mínimo, 2048 bits.

3.8.96. Para geração de hash, deve permitir a utilização do algoritmo SHA-256 ou variações superiores da família SHA-2.

3.8.97. Deve criptografar normalmente tráfego composto de quadros de 9000 bytes (jumboframe), sem realizar qualquer tipo de fragmentação do quadro.

3.8.98. Deve possibilitar a utilização de protocolos de roteamento que utilizam tráfego multicast, podendo esse tipo de tráfego ser encaminhado sem criptografia, se necessário.

3.8.99. O módulo de criptografia deverá preservar o cabeçalho Ethernet dos frames, assim mantendo os endereços MAC de origem e destino, além da identificação da VLAN associada a um determinado frame.

3.8.100. O processo de negociação de chaves de sessão entre os módulos de criptografia deverá ocorrer obrigatoriamente pelas interfaces destinadas para o fluxo de dados de produção, ou seja, não poderá ser feito pelas interfaces de gerência do equipamento.

3.8.101. O administrador deverá poder configurar o tempo de renegociação das chaves de sessão entre os módulos de criptografia, de modo que cada rekey possa ser realizado num período de tempo entre dez e sessenta minutos.

3.8.102. O equipamento deve possuir capacidade de instalação plug-and-play;

Licenciamento

3.8.103. Deve ser licenciado para um número de usuários e endereços IP ilimitados.

3.8.104. Quaisquer licenças necessárias para o funcionamento de todos os recursos e requisitos especificados nesse documento devem ser incluídas e não devem expirar após o término do tempo de vida de suporte dos equipamentos.

Certificações

3.8.105. O produto deve atender aos requisitos de segurança para módulos criptográficos definidos pelo padrão FIPS 140-2 Level 3, NATO E Common Criteria EAL2+

Segurança

3.8.106. O fabricante deve atestar e garantir formalmente que a solução não é passível de sofrer, por qualquer mecanismo ou método: acesso não autorizado, interceptação e monitoramento de comunicações de dados, por força de requerimentos legais ou regulatórios definidos por governos, agências, entidades ou pessoas.

3.9. **Garantia e suporte técnico**

3.9.1. A CONTRATADA deverá disponibilizar o canal de suporte técnico do fabricante, através de serviço telefônico, por no mínimo, 24x7 (vinte e quatro horas por dia, sete dias por semana), com atendimento, obrigatoriamente em língua portuguesa, falada no Brasil.

3.9.2. A CONTRATADA deverá fornecer suporte técnico do fabricante, no Brasil, obrigatoriamente em língua portuguesa, falada no Brasil para prestar atendimento e resolver todos os problemas relacionados às possíveis falhas ou interrupções de funcionamento da solução proposta, sempre que solicitado pelo CONTRATANTE;

3.9.3. A CONTRATADA deverá disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados do CONTRATANTE disponível em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados).

3.9.4. Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.

3.9.5. A CONTRATANTE poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência do contrato, para suprir suas necessidades com relação aos produtos de segurança.

3.9.6. Relatórios sobre a prestação dos serviços:

3.9.6.1. A CONTRATADA fornecerá relatório mensal, até o 10º (décimo) dia útil do mês subsequente ao serviço prestado, em arquivo eletrônico, preferencialmente em formato PDF, com informações analíticas e sintéticas sobre os serviços realizados no mês de referência, incluindo-se chamados abertos e fechados no período.

3.9.6.2. Constará dos relatório dados de todos os chamados ocorridos no período, incluindo data e hora de abertura do chamado, data e hora de início do atendimento, data e hora de fechamento do chamado, nome da pessoa que abriu o chamado, nome da pessoa que efetuou o atendimento, descrição do problema e descrição da solução.

3.9.7. Os atendimentos das ocorrências técnicas devem ser realizados em acordo com os critérios definidos pelos níveis de serviço da tabela abaixo, estando sujeita a CONTRATADA, no caso do descumprimento dos prazos, às sanções especificadas neste Termo de Referência:

Tabela 2 - Níveis de severidade

Severidade	Descrição	Prazo máximo para iniciar o Atendimento (em horas)
1	Problema técnico que impeça a utilização da solução em sua totalidade.	1h
2	Problema técnico que impeça a utilização parcial de uma funcionalidade, não impedindo por completo seu uso.	2h
3	Problema técnico que gere pouco ou baixo impacto na utilização da solução.	4h
4	Consulta técnica, dúvidas em geral, monitoramento,	8h

3.9.8. Sempre que o fabricante da solução disponibilizar versões mais atuais do software da solução oferecida, a CONTRATADA deverá disponibilizar essas versões, sem ônus adicionais, enquanto o contrato estiver vigente.

3.9.9. Os serviços deverão ser realizados por meio de técnicos especializados do fabricante, devidamente credenciados para prestar os serviços de garantia e suporte técnica remoto, de forma rápida, eficaz e eficiente, sem quaisquer despesas adicionais para o CONTRATANTE, inclusive quanto às ferramentas, equipamentos e demais instrumentos necessários à sua realização.

3.10. **Serviço de Instalação, Configuração e Implantação**

3.10.1. Os serviços técnicos especializados se mostram necessários para a garantia da efetiva implantação da solução adquirida. e compreendem as seguintes atividades:

3.10.1.1. Elaboração de plano de instalação, contendo todos os requisitos técnicos, etapas, prazos e matriz de responsabilidades.

3.10.1.2. Instalação física e energização da solução de criptografia de links e todos os módulos que a compõe, no ambiente disponibilizado pela CONTRATANTE.

3.10.1.3. Configurações necessárias para emissão de alertas através do sistema de correio eletrônico do CONTRATANTE.

3.10.1.4. Integração com NOC/SOC do CONTRATANTE.

3.10.2. Caberá ao CONTRATANTE disponibilizar o ambiente tecnológico para que a solução da CONTRATADA seja instalada e configurada.

3.10.3. O prazo máximo para a execução do serviço é de 30 (trinta) dias, a contar da data em que o CONTRATANTE disponibilizar o ambiente e credenciais de acesso para a execução da instalação e configurações.

3.10.4. A instalação deve ser realizada por profissionais especializados, que deverão possuir certificação do fabricante comprovando as habilidades técnicas necessárias para desempenhar atividades de instalação e configuração dos equipamentos e *software* adquiridos.

3.10.5. Ao término da execução do serviço, a CONTRATADA deverá elaborar um relatório com evidência de todo o processo de instalação e configuração. Deverá ainda ceder credenciais de acesso à equipe do CONTRATANTE.

3.10.6. A instalação e configuração da solução deverá ser realizada nas dependências do CONTRATANTE, e ocorrerá em ocorrer em dias úteis, no horário compreendido entre 9:00h e 18:00h, salvo definição contrária, realizada em comum acordo entre o CONTRATANTE e a CONTRATADA**.**

3.11. **Treinamento**

3.11.1. Deverá ser ofertado treinamento para a capacitação técnica de até 6 participantes selecionados pelo CONTRATANTE, com carga horária mínima de 16 (dezesseis) horas, material oficial do fabricante, e conteúdo necessários a capacitá-los para utilizar e gerenciar a Solução ofetada.

3.11.2. Deverá ser emitido certificado individual de participação ao final do curso.

3.11.3. Todo o material didático deve ser repassado de forma eletrônica para os participantes em até 48 (quarenta e oito horas) antes do início do curso.

3.11.4. Somente serão aceitos materiais oficiais dos fornecedores da Solução ofertada, e não será permitida a adaptação sobre apostilas/conteúdos de cursos não oficiais.

3.11.5. Os instrutores deverão possuir experiência em didática, além de possuir certificação comprovada na área de segurança, portanto pelo menos uma das seguintes certificações:

3.11.5.1. ISC2 CSSLP - Certified Secure Software Lifecycle Professional (ISO/IEC 17024);

3.11.5.2. ISC2 CISSP – Certified Information System Security Professional;

3.11.5.3. ISC2 ISSAP – Information System Security Architect Professional;

3.11.5.4. CISM – Certified Information Security Manager;

3.11.5.5. CompTIA Security+: Competency in system security, network infrastructure, access control and organizational security.

3.11.6. O treinamento deverá ocorrer nas dependências da CONTRATANTE, ou local por ela indicado na capital do estado, ficando ela responsável por montar o ambiente adequado para realização do mesmo, isto é, todo o espaço necessário assim como toda infraestrutura computacional e de rede necessária. Caberá à CONTRATADA viabilizar o acesso ao Sistema no ambiente de treinamento.

3.11.7. Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da CONTRATADA, incluindo os gastos com instrutores, seu deslocamento e hospedagem, a confecção e distribuição dos originais do material didático e a emissão de certificados para os profissionais treinados.

4. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

4.1. A presente seção contém o registro do quantitativo estimado de bens e serviços necessários para a composição da solução a ser contratada, de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo. Busca-se descrever também os métodos, as metodologias e as técnicas de estimativas que foram utilizados, nos termos do inciso I do art. 11 da IN SGD-ME n.º 01/2019.

4.2. Por se tratar de um registro de preços para atender todos os órgãos do governo federal integrantes do SISP, não há como se definir previamente o quantitativo total a ser adquirido. Essa resposta será obtida, com exatidão, quando da publicação da Intenção de Registro de Preços.

4.3. É importante lembrar que, em consonância com o princípio da economicidade, esta equipe de planejamento da contratação buscou elencar dois tipos de soluções tecnológicas a ser disponibilizadas para o CONTRATANTE. Tal medida busca atender tanto os órgãos públicos com uma maior infraestrutura de TIC quanto àqueles que possuem uma infraestrutura menor.

4.4. Alinhado com o parágrafo anterior e com vistas a possibilitar que cada órgão possa estabelecer a melhor alternativa para seu ambiente. Entendemos ser conveniente ofertar as opções de equipamentos de 1Gbps e 10Gbps. Está abordagem permiti que o órgão dimensione o tipo de *aplliance* com base no seu trafego de dados, porém é importante ressaltar que os equipamentos possuem os mesmos requisitos tecnológicos.

- **Opção 1 - *Appliance* TIPO 1 (portas 10Gbps)**
- **Opção 2 - *Appliance* TIPO 2 (portas 1Gbps)**

4.5. Considerando a arquitetura da solução, ou seja a necessidade de utilização do equipamento em cada ponta do link de dados, para fins dessa estimativa da demanda será considerado duas unidades de cada item.

4.6. Também contempla o escopo da pretensa contratação o serviço de instalação e implementação da *appliance* e um item relacionado a treinamento, com vista a operação e gerência dos equipamentos. Os itens 1 e 3 devem levar em consideração o suporte e garantia do fabricante por um período de 24 meses.

4.7. Abaixo a tabela de quantitativos estimativos iniciais:

Tabela 3 - Estimativa da Demanda

Item	Descrição	Quantidade
1	*Appliance* TIPO 1 (portas 10Gbps)	2
2	Serviços de instalação e Implementação de Appliance de Criptografia de Links TIPO 1	2
3	*Appliance* TIPO 2 (portas 1Gbps)	2
4	Serviços de instalação e Implementação de *Appliance* de Criptografia de Links TIPO 2	2
5	Treinamento para operação e gerência de *Appliances* TIPO 1 ou TIPO 2	1

4.8. Verifica-se que as quantidades acima são meramente aleatórias, com o objetivo de obter valores unitários de cada item. Após a abertura da IRP todos os órgãos do SISP interessados em participar, encaminharão os quantitativos reais para que possa ser consolidado a estimativa da demanda e posteriormente seja realizada uma nova cotação de preço a qual integrará a pesquisa de preço e consequentemente a definição do orçamento da licitação.

5. ANÁLISE DE SOLUÇÕES

5.1. Nesta seção, pretende-se apresentar os aspectos relacionados ao mercado fornecedor, apontando suas principais características e especificidades relacionadas às compras de governo nesse segmento.

5.2. A equipe de planejamento seguiu uma ordem lógica, que permitiu registrar todo o esforço empreendido até a escolha da solução que atende a demanda de forma mais eficiente.

5.3. Em primeiro lugar, a equipe de planejamento buscou entender o objeto junto ao segmento de mercado. Posteriormente, buscou avaliar as alternativas que se encontram disponíveis e por fim buscou avaliar qual o melhor modelo de fornecimento do objeto. A partir desses insumos, a equipe analisou todos os prós e contras e comparou com a demanda identificada pela área requisitante, o que permitiu concluir pelo cenário que atende às necessidades de forma mais eficiente.

5.4. **Segmentos de Mercado**

5.4.1. O mercado de segurança da informação no que tange a criptografia de link é restrito, não havendo muitos fabricantes que podem, a princípio, atender às demandas identificadas pela área requisitante.

5.5. **Identificação das soluções**

5.5.1. Observando-se as necessidades e os requisitos tecnológicos elencados nesse estudo técnico, bem como a análise do mercado, realizamos o levantamento das soluções relacionadas a criptografia de link e apresentamos uma descrição sucinta de cada uma delas.

5.5.2. Solução de Mercado 01 – AT Media

5.5.2.1. A atmedia GmbH foi fundada em 1996. A principal área da empresa é a comunicação de dados segura e confiável, a empresa possui as soluções Atmedia 1G Ethernet Encryptor e Atmedia 10G Ethernet Encryptor.

5.5.2.2. Solução de Mercado 02 – Rohde & Schwarz

5.5.2.3. Com mais de 30 anos de experiência em criptografia, a Rohde & Schwarz Cybersecurity é uma das pioneiras no campo de criptografia de rede com seu hardware e software de criptografia de rede, a empresa possui as soluções R&S®SITLine ETH e R&S®SITLine ETH NG

5.5.3. Solução de Mercado 03 – Securosys

5.5.3.1. A Securosys SA, fundada em 2014, com sede em Zurique, na Suíça, é uma empresa que atua no mercado em segurança cibernética, criptografia e proteção de identidades digitais a empresa possui a solução Securosys Centurion Network Encryptor.

5.5.4. Solução de Mercado 04 – Thales

5.5.4.1. Empresa francesa com mais de um século de existência e com mais de 50 anos de atuação no mercado brasileiro, a empresa possui a solução Encriptador de Rede Multilink Thales CN6140.

5.6. **Análise comparativa de soluções**

5.7. Segue abaixo a análise referente aos aspectos previstos na IN SGD-ME n. 01/2019 que devem ser avaliados em uma contratação de TIC.

Tabela 4 - Análise conforme IN n.º 01/2019

Requisito	**Solução**	**Sim**	**Não**	**Não se aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	AT Media		X	
	Rohde & Schwarz		X	
	Securosys		X	
	Thales	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	AT Media			X
	Rohde & Schwarz			X
	Securosys			X

	Thales			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	AT Media		X	
	Rohde & Schwarz		X	
	Securosys		X	
	Thales		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	AT Media			X
	Rohde & Schwarz			X
	Securosys			X
	Thales			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	AT Media			X
	Rohde & Schwarz			X
	Securosys			X
	Thales			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)	AT Media			X
	Rohde & Schwarz			X
	Securosys			X
	Thales			X

5.8. Complementamos o quadro acima com as seguintes informações acerca da solução considerada viável para o Ministério da Economia:

5.8.1. Necessidade de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual.

5.8.1.1. Não é necessário nenhuma adequação no ambiente do Ministério da Economia.

5.8.2. Possibilidade de aquisição na forma de bens ou contratação como serviço.

5.8.2.1. Foi definido pela equipe de planejamento da contratação que a aquisição ocorrerá mediante aquisição de bens, mediante despesa de capital.

5.8.2.2. De acordo com §1º do art. 9º do Decreto nº 7.174/2010 e §1º do art. 1º do Decreto nº 10.024/2019, esta licitação deve ser realizada na modalidade de Pregão, na sua forma eletrônica, com julgamento pelo critério de menor preço.

5.8.3. Parcelamento ou não da solução.

5.8.3.1. O objeto dessa contratação NÃO é passível de segmentação ou parcelamento. O parcelamento do objeto de acordo com a Lei deve ser feito em tantas parcelas quantas se comprovarem técnica e economicamente viáveis

5.8.3.2. A Solução Tecnológica pretendida é uma *appliance*, ou seja, um conjunto integrado em fábrica, de hardware e software que, juntos promovem alto desempenho, alta disponibilidade e segurança criptográfica de links.

5.8.3.3. O parcelamento das contratações de soluções de TI pelo Ministério da Economia é sempre ponderado em função do poder discricionário da Administração Pública, que lhe dá a prerrogativa de fazê-lo até o limite da coerência, da viabilidade técnica e da capacidade interna de gestão.

5.8.3.4. Neste caso, como já citado, o objeto em questão é uma *appliance* tecnicamente indivisível uma vez que todos os componentes de softwares e serviços são intrínsecos à mesma solução, não sendo possível o seu desmembramento.

5.8.4. Diferentes Tipos de Soluções em Termos de Especificação, Composição ou Características dos Bens e Serviços Integrantes

5.8.4.1. Não foram identificados outros tipos de solução relevantes além do exposto neste Estudo Técnico Preliminar.

5.8.5. Ampliação ou Substituição da solução implantada

5.8.5.1. Atualmente o Ministério da Economia não possui uma solução implantada que contemple o escopo dessa contratação, não cabendo ampliação ou substituição de solução.

5.8.6. Catálogos de Soluções de TIC com Condições Padronizadas

5.8.6.1. Ao analisar o Catálogo de Soluções de TIC com Condições Padronizadas (atualizado em 26/05/2022) "https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic, não foi identificado nenhum catálogo ativo com as fornecedoras analisadas nesse estudo ETPC.

5.9.

6. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

6.1. As soluções dos fornecedores AT Media e Securosys, em função de não existir representação desses fabricantes de forma direta ou mediante revendas no território nacional.

6.2.

7. ANÁLISE E IDENTIFICAÇÃO DE SOLUÇÕES VIÁVEIS DE MERCADO

7.1. Considerando a análise realizada no tópico 5 - ANÁLISE DE SOLUÇÕES, a equipe de planejamento da contratação entende que a melhor solução tecnológica será definida em **disputa de mercado com garantia a ampla concorrência dos fabricantes com representatividade no Brasil, desde que atendam as especificações técnicas requeridas**.

8. ANÁLISE COMPARATIVA DE CUSTO TOTAL (TCO)

8.1. A equipe de planejamento da contratação não realizou a análise comparativa de custos em virtude do estudo técnico preliminar da contratação identificar somente uma solução/cenário viável, conforme disciplina o inciso III do art. 11 da IN SGD/ME nº 01/2019:

> "III - A análise comparativa de custos deverá considerar apenas as soluções técnica e funcionalmente viáveis, incluindo:"

9. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

9.1. Diante da análise de mercado, alinhando-se aos objetivos de negócio e ao perfil de demanda registrada, foi constatado que a melhor solução tecnológica será definida em **disputa de mercado com garantia a ampla concorrência dos fabricantes com representatividade no Brasil, desde que atendam as especificações técnicas requeridas nesse ETPC.**

10. ANÁLISE DA INTENÇÃO DE REGISTRO DE PREÇO

11. ESTRATÉGIA DA CONTRATAÇÃO

11.1. A presente seção descrever os estudos e justificativas que fundamentaram decisões na modelagem de diferentes aspectos e condições do Termo de Referência.

11.2. Vigência e modalidade da licitação

11.2.1. Por se tratarem de serviços comuns, o objeto da presente licitação deve ser licitado na modalidade PREGÃO ELETRÔNICO, com adjudicação pelo valor global.

11.2.2. O contrato deverá ter vigência de 24 meses podendo ser prorrogado por igual período conforme estabelece o art.57 da lei 8.666.93.

11.3. Justificativa para vigência superior a 12 meses

11.3.1. O artigo 57 da Lei Federal nº 8.666/93 disciplina a duração dos contratos administrativos, bem como as possíveis hipóteses de prorrogação de seu prazo de vigência.

> ***Art. 57. A duração dos contratos regidos por esta Lei ficará adstrita à vigência dos respectivos créditos orçamentários, exceto quanto aos relativos:***
> ***I - aos projetos cujos produtos estejam contemplados nas metas estabelecidas no Plano Plurianual, os quais poderão ser prorrogados se houver interesse da Administração e desde que isso tenha sido previsto no ato convocatório;***
> ***II - à prestação de serviços a serem executados de forma contínua, que poderão ter a sua duração prorrogada por iguais e sucessivos períodos com vistas à obtenção de preços e condições mais vantajosas para a administração, limitada a sessenta meses;***
> ***III - (Vetado).***
> ***IV - ao aluguel de equipamentos e à utilização de programas de informática, podendo a duração estender-se pelo prazo de até 48 (quarenta e oito) meses após o início da vigência do contrato.***
> ***V - às hipóteses previstas nos incisos IX, XIX, XXVIII e XXXI do art. 24, cujos contratos poderão ter vigência por até 120 (cento e vinte) meses, caso haja interesse da administração.***

11.3.2. A regra estabelecida pelo artigo 57 se mostra bem clara: a duração dos contratos, em regra, deve se restringir à vigência dos respectivos créditos orçamentários, restando vedado o contrato administrativo com prazo de vigência indeterminado.

11.3.3. Não existe vedação nenhuma quanto a definição da vigência contratual no Art. 57 da Lei 8.666/1993 estar acima de 12 meses. Pelo contrário, ele autoriza que um contrato de serviço continuado seja vigente por até 60 meses.

11.3.4. Quanto a adoção de prazo de vigência da contratação ser de 24 (vinte e quatro) meses, prorrogável até o limite de 60 (sessenta) meses, esclarecermos que um período de vigência contratual ampliado contribui para que a contratação em tela possa ser considerada mais atrativa pelo mercado por meio de uma maior diluição dos custos com depreciação e manutenção dos equipamentos ou investimentos, o que pode, inclusive, ter impactos sobre o preço final proposto pela licitante vencedora do certame, favorecendo a Administração em termos de economicidade e ampliação da competitividade.

11.3.5. Seguindo esta lógica, a jurisprudência do TCU sustenta a possibilidade da fixação do prazo de vigência estendido com a finalidade de obter preços e condições mais vantajosos para a Administração, como o Acórdão 3.320/2013-Segunda Câmara:

> ***"O prazo de vigência de contratos de serviços contínuos deve ser estabelecido considerando-se as circunstâncias de forma objetiva, fazendo-se registrar no processo próprio o modo como interferem na decisão e quais suas consequências. Tal registro é especialmente importante quando se fizer necessário prazo inicial superior aos doze meses entendidos como regra pelo TCU. Há necessidade de se demonstrar o benefício decorrente do prazo estabelecido (Acórdão 3320/2013-Segunda Câmara)."***

11.3.5.1. No caso em questão a contratação com previsibilidade de vigência acima dos 12 meses é econômica e tecnicamente mais vantajosa para a Administração, conforme vantagens elencadas abaixo:

- Evitar o acionamento da máquina pública a cada prorrogação;
- Evitar gastos administrativos nessas autuações a cada 12 meses;
- Possibilidade de diluir investimentos ou de custos por parte do particular (amortização), facilitando o dimensionamento do investimento, afetando significativamente os valores mensais do contrato;
- Atender às características específicas da contratação;
- Reduzir a complexidade de implementação da solução para um período de vigência maior;
- Alterar a cultura diária dos usuários da instituição envolvendo alteração de processos e curva de aprendizado, que nos casos de 12 meses gera um impacto ainda mais oneroso;
- Aumento da capacidade de segurança através da integração com as demais soluções da instituição que irão demandar maior esforço, pois perpetuando por um período maior, reduz riscos elevados à segurança; e
- Ganhos de economicidade.

11.4. Estimativa da Demanda

11.4.1. A estimativa de demanda será realizada após consulta a todos os órgãos integrantes do SISP.

11.4.2. Não existe, neste primeiro momento, possibilidade de definir com elevado grau de precisão, qual o quantitativo exato a ser contratado. De qualquer forma, como o objetivo desse projeto é a disponibilização da solução para os integrantes do SISP, sugere-se a adoção do sistema de registro de preços para satisfazer a presente demanda.

11.4.3. A adoção do sistema de registro de preço justifica-se pela forma de aquisição dos bens e serviços, que terá previsão de entregas parceladas, segundo a nossa necessidade, conforme as disponibilidades orçamentárias, uma vez que segundo Decreto nº 7.892/2013:

> ***"Art. 2º Será adotado, preferencialmente, o SRP nas seguintes hipóteses:***
> ***I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;***
> ***II - quando for mais conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços necessários à Administração para o desempenho de suas atribuições;***
> ***[...]***
> ***IV - quando pela natureza do objeto não for possível definir previamente o quantitativo a ser demandado pela Administração."***

12. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

12.1. A estimativa de custos da contratação considerou a contratação de 100% do volume projetado no item 4 - ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS. Dessa forma, tem-se a seguinte estimativa de custos

Tabela 5 - Estimativa de custos da contratação

ITEM/FORNECEDOR	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
Appliance de Criptografia de Links TIPO1	Hardware	2	R$ 1.014.585,00	R$ 2.029.170,00
Serviços de instalação, configuração e implantação de Appliance de Criptografia de Links TIPO 1	Serviço	2	R$ 39.586,51	R$ 79.173,02
Appliance de Criptografia de Links TIPO2	Hardware	2	R$ 580.364,00	R$ 1.160.728,00
Serviços de instalação, configuração e implantação de Appliance de Criptografia de Links TIPO 2	Serviço	2	R$ 39.586,51	R$ 79.137,02
Treinamento para operação e gerência de Appliances Serviço 1 (TIPO 1 ou TIPO 2)	Serviço	1	R$ 107.000,00	R$ 107.000,00
Valor Total de Referência				**R$ 3.405.244,04**

12.2. Esta estimativa será melhor detalhada após a finalização da Intenção de Registro de Preço (IRP). Após isso, será realizada pesquisa de preços e a estimativa será consolida com os volumes finais e os valores unitários na versão final do Termo de Referência. Vide pesquisa de preços e versão final do TR.

13. DO MODO DE DISPUTA DO PREGÃO

13.1. A presente seção define e justifica o modo de disputa a ser adotado no Pregão, em atenção ao Decreto 10.024, de 20 de setembro de 2019. Inicialmente, destaca-se que o referido Decreto introduziu a figura do modo de disputa a ser adotado no pregão, podendo ser aberto (descrito no art. 32 desse Decreto) ou aberto e fechado (descrito no art. 33 desse Decreto).

13.2. Os modos de disputa definem como se dará o envio de lances no pregão eletrônico. No modo aberto, os licitantes apresentarão lances públicos e sucessivos, com prorrogações, conforme o critério de julgamento adotado no edital. Já no modo Aberto e Fechado, os licitantes apresentarão lances públicos e sucessivos, com lance final fechado.

13.3. Para se definir o modo de disputa mais apropriado para a presente contratação, observou-se as seguintes características inerentes à Teoria do Leilões, conforme descrita em vasta bibliografia relacionada a essa Teoria, em específico na obra de Paul Klemperer, "What Really Matters in Auction Design", publicação realizada no Journal of Economic Perspectives -Volume 16, Number 1 páginas 169–189 (Disponível neste link):

a. Propensão à colusão; e
b. Prevenção ao comportamento predatório.

13.4. Ressalta-se, inicialmente, que cada modo de disputa possui características específicas que os tornam mais ou menos vantajosos a depender das condições relacionadas à estrutura do mercado, à natureza do objeto e ao arranjo local de fornecimento dos bens e serviços. Note que a vantajosidade a ser perseguida relaciona-se a maior quantidade de incentivos que o modo de disputa é capaz de fornecer para que o desenho do mecanismos de seleção do fornecedor possibilite o alcance do melhor resultado para a administração, mitigando-se o risco da ocorrência de disfunções entre os agentes participantes que afetem a ampla concorrência e o melhor preço à administração pública.

13.5. Sobre a propensão à colusão, verificou-se no presente estudo que existe pouco fabricantes estabelecidos no território nacional que possuem soluções que atendam os requisitos definidos nesse estudo técnico, consequentemente o setor de venda para o governo desse tipo de produto acompanha um nível de concentração elevado. Em mercados altamente concentrados, a probabilidade da ocorrência da colusão explícita ou tácita é maior. Nesse sentido, a utilização de uma fase de lances selados, segundo Klemperer, é mais apropriada para mitigar o risco de colusão, principalmente porque evita a chamada sinalização de propostas (Bid Signaling).

13.5.1. Outro aspecto a ser considerado é o grau de padronização ou homogeneização do produto objeto da contratação. Isso porque produtos diversificados permitem que diferentes fornecedores assumam um comportamento prejudicial à concorrência, denominado de comportamento predatório, ou seja, assumam lances próximos à inexequibilidade com o intuito de criar artificialmente barreiras à entrada de novos participantes. Por se tratar de uma solução nomeada, o modelo de disputa mais adequado é aquele que possua uma fase de propostas seladas, uma vez que o risco de ocorrência da chamada maldição do fornecedor ou de eventual risco moral é menor do que em casos de produtos muitos diversificados.

13.5.2. Pelo exposto, e considerando ainda o número não expressivo de prestadores dos serviços em vendas para o governo devido ao grau de concentração, o modo de disputa do Pregão deverá ser ABERTO E FECHADO, conforme rito estabelecido no artigo 33 do Decreto nº 10.024, de 2019, que regulamenta a licitação, na modalidade de pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da Administração Pública Federal.

14. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

14.1. A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

14.2. Nesse sentido, o planejamento em tela almeja os seguintes resultados:

- Economia no valor da licitação em função do ganho de escala e na forma agrupada de contratação;
- Eficiência com a redução do custo administrativo em função do agrupamento de itens em uma solução única;
- Efetividade com a padronização dos itens previstos, subscrições e aumento da qualidade das especificações técnicas; e
- Eficácia com o atendimento das necessidades de diversas instituições referente a solução de Criptografia de link de dados.

14.3. Além disso, frisa-se que a presente contratação atende adequadamente às demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis.

14.4. Considerando as informações do presente estudo, entende-se que a presente contratação se configura econômica e tecnicamente **VIÁVEL**

15. APROVAÇÃO E ASSINATURA

15.1. Equipe de Planejamento da Contratação instituída pelo Documento de Oficialização de Demanda (SEI-ME 24531798) e Despacho SGES-CNTRAL-CGTIC (SEI-ME 24778931) .

15.2. Estudo Técnico Preliminar aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC, conforme o § 2º do Art. 11 da IN SGD-ME nº 01, de 2019.

Documento assinado eletronicamente

FÁBIO MORETH MARIANO

Integrante Técnico

Matrícula/SIAPE: 1793489

Documento assinado eletronicamente

ELEIDMAR ODILIA ISAQUE DA SILVA

Integrante Requisitante

Matrícula/SIAPE: 1774903

Aprovo.

Documento assinado eletronicamente

LARA BRAINER MAGALHÃES TORRES DE OLIVEIRA

Diretora

Matrícula/SIAPE 1503583