**RFP**

Diretoria de Operações

Redes Privativas do Governo

Requisitos

Funcionalidade de Criptografia - Encriptadores

Rede Privativa do Governo

[1. Descrição do Projeto da Rede Privativa de Governo 3](#_Toc208242551)

[2. Descrição dos Serviços / Produtos 6](#_Toc208242552)

[3. Requisitos 7](#_Toc208242553)

[3.1. Requisitos de Documentação 7](#_Toc208242554)

[3.2. Arquitetura da Rede 8](#_Toc208242555)

[3.3. Requisitos Técnicos 11](#_Toc208242556)

[3.3.1. Encriptadores de Enlace 11](#_Toc208242557)

[3.3.2. Licenciamento – Suporte e garantia do produto 20](#_Toc208242558)

[3.3.3. Políticas e alinhamentos de segurança da informação: 21](#_Toc208242559)

[3.3.4. Roadmap de Hardware e Software: 21](#_Toc208242560)

[3.3.5. Gerenciamento de Falhas (FM) 22](#_Toc208242561)

[3.3.6. Gerenciamento de Configuração (CM) 24](#_Toc208242562)

[3.3.7. Gerenciamento de Performance (PM) 26](#_Toc208242563)

[3.3.8. Certificado de conformidade 27](#_Toc208242564)

[3.3.9. Sobressalentes 27](#_Toc208242565)

[3.3.10. Requisitos de Manutenção e Suporte Operacional 27](#_Toc208242566)

[3.3.11. Desenvolvimento de Competências e Transferência de Conhecimento 28](#_Toc208242567)

[3.3.12. Embarque de Algoritmo de Criptografia do Estado Brasileiro 29](#_Toc208242568)

[4. Serviços 31](#_Toc208242569)

[4.1. Projeto 31](#_Toc208242570)

[4.2. Entrega de Equipamentos 31](#_Toc208242571)

[4.3. Instalação; 31](#_Toc208242572)

[4.4. Comissionamento, Integração e Testes 32](#_Toc208242573)

[4.5. Aceitação 33](#_Toc208242574)

[4.6. Gerência de Projeto 34](#_Toc208242575)

# Descrição do Projeto da Rede Privativa de Governo

1. Esse capítulo tem o objetivo de contextualizar a PROPONENTE sobre a Rede Privativa de Governo, a qual deverá ser protegida, de acordo com o projeto específico para cada cliente, pela solução de **Encriptadores**, escopo dessa RFP.
2. A **Rede Fixa Privativa** terá atendimento de até 6.500 pontos nas **Capitais** em dupla abordagem, com capacidade de atendimento conforme a necessidade de banda do usuário ( 1Gbps, 10Gbps e 100Gbps) não se limitando a estas bandas, utilizando interfaces ETHERNET, GPON e XGS-PON. A rede fixa será implementada em todas as 26 capitais do Brasil e o Distrito Federal, utilizando o backbone da TELEBRAS bem como a sua estrutura de fibra óptica já lançada nas capitais, sendo esta nova rede um complemento da rede existente.

Diagrama

Descrição gerada automaticamente

Figura 1 - Arquitetura da Rede Fixa

1. A rede de transporte será formada por roteadores e switches interconectados em anéis redundantes de fibra óptica, a fim de prover a comunicação entre a rede fixa de acesso e o backbone de dados da TELEBRAS.
2. A rede SD-WAN será formada utilizando elementos da rede de transmissão implementada pela EAF e/ou rede de transmissão existentes de outras operadoras, como redes móveis (4G/5G), satélite, rede fixa etc. Tais elementos serão gerenciados por um elemento orquestrador de hierarquia superior instalado em um datacenter centralizado visando prover o uso mais eficiente dos recursos disponíveis da rede.

Diagrama

Descrição gerada automaticamente

Figura 2 - Arquitetura da Rede SD-WAN exemplificando a utilização dos up-links

1. **Atendimento de** **pontos fora das capitais**: além dos pontos nas capitais, que fazem parte da Rede Privativa, os encriptadores também poderão ser instalados em pontos fora das capitais, visando ampliar a proteção na rede dos clientes. Nesses pontos fora das capitais, o encriptador será inserido na rede do cliente e deve funcionar de forma agnóstica ao tipo de rede. Abaixo a topologia para o atendimento fora das capitais:

Diagrama

O conteúdo gerado por IA pode estar incorreto.

Figura 3 – Topologia para atendimento com encriptadores fora das capitais

1. Considerando as arquiteturas das redes que precisam ser protegidas, segue abaixo resumo com informações gerais do projeto nominal para o fornecedor dos Encriptadores ter uma ideia do requisito:

|  |  |
| --- | --- |
| Plano Nominal |  |
| Infraestrutura a ser Protegida | Pontos da Rede Privativa Fixa nas Capitais com Enlaces SD-WAN;  Pontos atendidos fora das Capitais, que não pertencem a Rede Privativa Fixa (sem SD-WAN). |
| Funcionalidade de Criptografia | * Encriptadores de Enlace; * HSM para gerenciamento dos certificados e chaves criptográficas; * Gerência unificada da solução; * Ferramenta para embarque e controle do algoritmo de Estado Brasileiro. |

Tabela 1 - Plano de Projeto Nominal

|  |  |
| --- | --- |
| Traffic Model |  |
| Encriptadores de Enlace | O sistema deve ter capacidade para Encriptar 6500 Enlaces;  Capacidade para Encriptar/Decriptar 1Gbps, 10Gbps e 100Gbps  Suporte à Algorítimo de Cripografia do Governo  Estimativa de Encriptadores de Enlace por Região |

Tabela 2 - Modelo para dimensionamento da Solução



Tabela 3 - Estimativa de Encriptadores por Região

# Descrição dos Serviços / Produtos

1. As PROPONENTES devem fornecer, no mínimo, uma proposta completa para o escopo descrito abaixo.
2. Esta RFP se concentrará especificamente nas **Soluções de Encriptadores de Enlace** para a Funcionalidade de Criptografia para a Rede Privativa do Governo.
3. Especificamente, esse documento abrange:
   * 1. Os equipamentos e softwares para a a Solução de Criptografia, funções de suporte, sistema de gerenciamento de elementos, interfaces e arquitetura.
     2. Equipamentos e software para fins de sistema de gerenciamento da Solução.
     3. Serviços de suporte à solução, incluindo garantia, manutenção e suporte L3.
     4. Requisitos de suporte operacional, incluindo peças de reposição, logística, suporte a serviços gerenciados e transferência de competências.
     5. Desenvolvimento de documentação operacional para práticas recomendadas, incluindo processos, *troubleshooting* e *runbooks* detalhados.
     6. Softwares de Segurança e gerenciamento de *firmware* (Identificar, testar e lançar)

Além disso, a PROPONENTE também pode apresentar sua proposta para o Escopo Opcional, se for qualificada. RFPs separadas serão lançadas pela EAF para outras funções de rede e plataformas.

# Requisitos

1. A solução proposta pela PROPONENTE deve atender a todos os requisitos mandatórios da Statement of Compliance (SoC) ao longo deste documento.
2. Além disso, existem requisitos que são específicos para a resposta da PROPONENTE.
3. A resposta da PROPONENTE deve descrever como todos os requisitos de SOW serão atendidos pela solução proposta e deve atender a todos os requisitos mandatórios de RFP.
4. É facultado à EAF flexibilizar ou não requerimentos, considerados inicialmente como mandatórios, em caso de atendimento parcial (Parcialmente em Conformidade), ou não atendimento (Não Conforme), desde que a resposta e ou explicação da PROPONENTE evidencie que não haverá impacto negativo no projeto.

# Requisitos de Documentação

1. A PROPONENTE deve fornecer documentação para as funções de software e plataformas de hardware, incluindo a descrição do produto, descrição funcional, descrição das interfaces, da arquitetura, diagrama esquemático, layout da placa de circuito impresso (PCB) e fotografias do equipamento. Além disso, os códigos fonte de software e firmware devem ser disponibilizados para verificação de órgão de segurança da administração pública federal.
2. A PROPONENTE deve fornecer relatórios de teste confirmando a conformidade com as normas exigidas e a documentação necessária atestando a homologação no Brasil (Anatel).
3. A PROPONENTE deve fornecer documentação para dar suporte aos serviços de implantação e operações, incluindo um guia de Dimensionamento, um guia de Instalação, Configuração e Comissionamento, bem como um guia de Operação e Manutenção.
4. A PROPONENTE deve apresentar no mínimo os seguinte documentação:
5. Documento de descrição detalhada da solução técnica;
6. Arquitetura e descrição do sistema;
7. Relação de todos os elementos/funcionalidades oferecidos na proposta, com suas respectivas capacidades;
8. Descrição do produto;
9. Descrição das Features;
10. Casos de usuários, fluxos de chamadas, fluxo de serviço;
11. Instalação de hardware e software;
12. Documentos de configuração;
13. Resolução de problemas (*Troubleshooting*) e código de erro;
14. Contadores e estatísticas;
15. Relatórios de KPI;
16. Descrição de parâmetros;
17. Certificados de Homologação;

# Arquitetura da Rede

Esta seção descreve a arquitetura da Rede Privativa da EAF, a qual deverá ser protegida pelas ferramentas e soluções requisitadas nessa RFP:

1. Arquitetura SD-WAN

Diagrama

Descrição gerada automaticamente

Figura 4 - Arquitetura SD-WAN

1. A solução deverá ser flexível para suportar todas as Arquiteturas/Topologias elencadas abaixo:
   1. **Topologia com Encriptador na interface WAN do SD-WAN:** 
      1. O encriptador deve possuir funcionalidade de filtros para que apenas o tráfego de interesse seja criptografado. Deve ser possível aplicar filtros de acordo com os destinos (IP e Porta), com o protocolo e com a VLAN, nas camadas 3 ou 4.
      2. O encriptador deve ter a capacidade de encriptar o payload (a partir da camada 3 ou 4) sem a necessidade de estabelecer um túnel IPSEC, pois o tráfego já será encapsulado pelo túnel IPSEC do SD-WAN.

Diagrama

Descrição gerada automaticamente

Figura 5 - Arquitetura Encriptadores de Enlace na Interface WAN do SD-WAN

* 1. **Topologia com Encriptador em paralelo com o SD-WAN:**
     1. o encriptador deve ter a capacidade de encriptar o payload (a partir da camada 3 ou 4) sem a necessidade de estabelecer um túnel IPSEC, pois o tráfego já será encapsulado pelo túnel IPSEC do SD-WAN.

Diagrama

Descrição gerada automaticamente

Figura 6 - Arquitetura Encriptadores de Enlace em Paralelo com o SD-WAN

* 1. **Topologia híbrida:**
     1. O encriptador deve possuir funcionalidade de filtros para que apenas o tráfego de interesse seja criptografado. Deve ser possível aplicar filtros de acordo com os destinos (IP e Porta), com o protocolo e com a VLAN, nas camadas 3 ou 4.
     2. O encriptador deve ter a capacidade de encriptar o payload (a partir da camada 3 ou 4) sem a necessidade de estabelecer um túnel IPSEC, pois o tráfego já será encapsulado pelo túnel IPSEC do SD-WAN.

Diagrama

Descrição gerada automaticamente

Figura 7 - Arquitetura Encriptadores de Enlace Híbrida

* 1. **Topologia para atendimento fora das capitais:** 
     1. O encriptador deve possuir funcionalidade de filtros para que apenas o tráfego de interesse seja criptografado. Deve ser possível aplicar filtros de acordo com os destinos (IP e Porta), com o protocolo e com a VLAN, nas camadas 3 ou 4.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

Figura 8 - Arquitetura Encriptadores fora das Capitais

# Requisitos Técnicos

# Encriptadores de Enlace

* + - 1. O encriptador de rede é a segurança aplicada à rede de uma organização para proteger e controlar esses dados internamente. A criptografia da camada de rede envolve criptografar dados à medida que são enviados de um nó e descriptografá-los na chegada em outro, por requimento do edital da Anatel essa criptografia deve usar algoritmo de origem proprietária do governo brasileiro.
      2. Os Encriptadores devem fazer a proteção da Comunicação entre as eNodeb e o CORE EPC, a comunicação entre os órgãos atendidos pela rede fixa, assim como os elementos da rede SD-WAN.
      3. A PROPONENTE deve descrever em detalhes como é a interoperabilidade do Encriptador com elementos SD-WAN. Ou seja, qual a topologia sugerida para que o encriptador possa ser utilizado sem que o SD-WAN perca suas funcionalidades.
      4. Ao ser posicionado na interface WAN do SD-WAN, o Encriptador deve ser capaz de apenas criptografar o payload, sem a necessidade de estabelecer um novo túnel IPSEC, considerando que o SD-WAN já estabelecerá este túnel antes do tráfego chegar no Encriptador.
      5. A solução deve ser independente do provedor do serviço de telecomunicações, e agnóstica em relação ao tráfego transportado, tais como, rede IP ou rede MPLS, transmissão satelital ou terrestre;
      6. A solução deve fornecer possibilidade de encriptar o tráfego a partir das camadas 2, 3 ou 4.
      7. A solução deve fornecer possibilidade de gerenciamento de regras para escolha do tipo de tráfego a ser criptografado. As regras devem considerar a possibilidade de encriptar, ou não, de acordo com os destinos (IP e Porta), com o protocolo e com a VLAN, nas camadas 2, 3 ou 4.
      8. Ao criptografar o payload, o Encriptador deve preservar as marcações de QoS presentes nas chamadas 2, 2,5 e/ou 3.
      9. A solução deve ser composta pelos Encriptadores, Autoridade Certificadora de Equipamentos para sigilo, módulos de segurança em hardware (HSM), ferramentas de embarque de algoritmos criptográficos e console de gestão;
      10. A solução deve permitir o embarque de suíte de algoritmos criptográficos proprietários definidos pela EAF, como o algoritmo de Estado Brasileiro, e o uso simultâneo de suítes;
      11. Deve suportar a criação de tuneis Layer-3 entre entre interface ethernet LAN de dois terminadores VPNs distintos, através de endereços WAN IPv4 ou IPv6 roteáveis entre si (sem NAT);
      12. Deve suportar a criação de tuneis Layer-3 entre entre interface ethernet LAN de dois terminadores VPNs distintos, através de endereço WAN IPv4 público no terminador A e WAN IPv4 privado, passando por infraestrutura de NAT Hide para IP privado, no terminador Z;
      13. Deve suportar encapsular qualquer pacote IPv4 e IPv6 dentro de túneis Layer-3, com túnel estabelecido entre IPv4 (WAN) ou IPv6 (WAN);
      14. Deve suportar a configuração de tunéis Layer3 em topologia full mesh, com cada terminador de VPN criando túneis com todos os outros terminadores VPN e encaminhando os pacotes IPv4 / IPv6 diretamente para o tunel associado ao terminador VPN com a LAN de destino;
      15. Deve suportar a configuração de tunéis Layer3 em topologia hub spoke, com um terminador VPN atuando como HUB, e com a criação de túneis apenas entre o terminador HUB e os outros terminadores VPNs (spokes). O terminador HUB deverá rotear o tráfego originado em um terminador spoke com destino a outro terminador spoke que será encaminhado ao hub;
      16. Deve suportar o estabelecimento de tunel criptográfico layer-3 em modo TUNEL, com encapsulamento total do pacote ip original;
      17. Deve suportar o estabelecimento de tunel criptográfico layer-3 em modo TRANSPORTE, com encapsulamento apenas do payload do pacote IP, e preservando as marcações de QoS camada 2, 2,5 e 3;
      18. Deve suprotar o roteamento de pacotes IPv4 / IPv6 tanto por dentro dos túneis criptografados quanto por roteamento convencional, sem criptografia, se a rede LAN de destino ainda não possuir terminador de VPN;
      19. Deve suportar a criação de listas de acessos por prefixos IPv4 / IPv6, / VRFs de origem e destino associando as mesmas ao direcionamento do pacote ip para um determinado tunel criptografico ou então via roteamento convencional, sem criptografia;
      20. Deve suportar a configuração de hostname, syslocation, data, hora, timezone;
      21. Deve implementar cliente NTP para sincronização de relógio e acurária dos registros de log;
      22. Deve implementar syslog local e remoto, permitindo a configuração de múltiplos servidores de syslog, e audit trail local para análise post-morten;
      23. A solução deve ser composta por equipamentos de rede responsáveis pela segurança da comunicação e de uma solução de gestão dos equipamentos.
      24. A solução de gestão deve ser totalmente integrada ao equipamento utilizado e permitir a configuração e monitoramento remoto de todos os equipamentos.
      25. O sistema de gestão deve apresentar dashboard que dê ao operador a visão geral da operação dos equipamentos, assim como possibilidade de detalhar e filtrar informações (alarmes, erros, etc).
      26. A solução deve conter recurso para configuração em massa dos equipamentos.
      27. A PROPONENTE deve apresentar uma visão geral da solução, descrevendo todos os elementos necessários para o seu funcionamento, assim como o hardware e o software;
      28. A PROPONENTE deve informar se a solução se baseia em códigos abertos, descrevendo-os e informando suas respectivas versões;
      29. A solução deve ser baseada em protocolos abertos de mercado, podendo conter modos proprietários de operação. O uso de protocolo aberto deve permitir a interoperabilidade com soluções de terceiros, com níveis de performance, estabilidade e recursos típicos do mercado.
      30. A PROPONENTE deve descrever como a solução pode interoperar com outras soluções de VPN;
      31. Geração de Números Aleatórios:
          1. A solução deve conter um gerador de números verdadeiramente aleatórios dedicado, em específico o gerador deve satisfazer a todos os requisitos necessários para ser classificado como Classe de Funcionalidade PTG.3, descrita no documento AIS 31 do BSI.
          2. A PROPONENTE deve informar se o RNG possui certificação.
          3. A PROPONTENTE deve descrever a arquitetura de Geração de Números Aleatórios (Random Number Generator - RNG), especificando todos os componentes, hardware e software.
          4. Os geradores aleatórios devem ser capazes de passar nos testes do NIST (SP 800-22) e nos testes do Dieharder (Rober G.Brown). Deve ser possível a extração de 1 GiB para que se possa fazer análise estatística dos bits.
          5. A solução deve permitir a inserção de entropia externa.
          6. A PROPONENTE deve descrever o procedimento de monitoramento da qualidade da entropia do RNG.
      32. Criptografia Assimétrica:
          1. A PROPONENTE deve descrever os algoritmos assimétricos disponíveis em hardware ou software.
          2. A solução deve conter algoritmos assimétricos clássicos, como RSA-2048 (ou de maior segurança) e curvas elípticas padronizadas pelos NIST de, ao menos, 256-bits.
          3. O solução deve disponibilizar ao menos uma curva elíptica de 521-bits.
          4. A PROPONENTE deve informar como são adicionadas novas curvas elípticas em hardware e/ou software.
          5. A PROPONENTE deve descrever os algoritmos pós-quânticos aprovados pelo NIST disponíveis em hardware e/ou software.
          6. A solução deve conter algoritmos assimétricos pós-quânticos em padronização pelo NIST: CRYSTALS-Kyber e pelo menos um de assinatura.
          7. Todas as opções de segurança dos algoritmos pós-quânticos selecionados devem estar disponíveis.
          8. A solução deve ser capaz de importar curvas elípticas customizadas no padrão OpenSSL e disponibilizar para todos os equipamentos automaticamente.
          9. A PROPONENTE deve descrever quais protocolos híbridos o sistema permite a utilização (combinação da criptografia assimétrica clássica com a pós-quântica).
          10. A PROPONTENTE deve detalhar como adicionar novos algoritmos em hardware e/ou software.
      33. Criptografia Simétrica:
          1. A PROPONENTE deve descrever os algoritmos criptográficos simétricos embarcados em hardware.
          2. A PROPONENTE deve descrever os algoritmos criptográficos simétricos disponíveis em software.
          3. A solução deve conter o algoritmo simétrico AES256-GCM.
          4. A solução deve permitir inserção de algoritmos proprietários.
          5. A PROPONENTE deve descrever como o sistema permite embarcar criptografia simétrica proprietária em software.
          6. A PROPONENTE deve descrever como o sistema permite embarcar criptografia simétrica proprietária em hardware.
          7. A solução deve ser capaz de importar ou integrar algoritmo simétrico customizável de 512-bits de bloco baseado em arquitetura ARX, família Salsa-Chacha.
      34. Gestão das Chaves Criptográficas
          1. As chaves criptográficas devem ser armazenadas em um perímetro criptográfico e seu uso não deve ser realizado fora deste perímetro.
          2. A gestão das chaves criptográficas e seu ciclo de vida deve ser feita de forma centralizada e com alta disponibilidade;
          3. A solução oferecer um HSM para o armazenamento e gestão das chaves criptográficas utilizada pelos Encriptadores.
          4. A PROPONENTE deve informar se o HSM da solução é capaz de interoperar com elementos SDWAN fornecendo solução segura para o armazenamento e gestão das chaves criptográficas utilizadas na rede SDWAN.
          5. O HSM deve possuir certificação FIPS 140-3 nível 3.
          6. O HSM deve ser instalado no datacenter da Rede Privativa de Governo.
          7. As chaves criptográficas devem ser armazenadas cifradas.
          8. A chave utilizada para cifrar as chaves armazenadas em memória deve ser derivada, utilizando-se uma senha e um salt como parâmetros de entrada do protocolo Argon2 ou PBKDF2
          9. As chaves criptográficas devem ser geradas dentro do perímetro criptográfico.
          10. Deve ser empregado protocolo de apagamento seguro para destruição das chaves, impossibilitando a recuperação da chave através de técnicas lógicas e físicas.
          11. O sistema deve ser resiliente a interrupções pontuais do processo de geração das chaves, exemplo, via queda de energia, ou via comando do usuário.
          12. O sistema deve prover meios de configuração que permitam especificar, durante o processo de geração, que uma chave não deve ser extraída logicamente em nenhuma hipótese.
      35. Autenticação para fechamento de túnel entre equipamentos
          1. A PROPONENTE deve descrever o protocolo utilizado para que os equipamentos se autentiquem.
          2. A solução deve ter a capacidade de utilizar certificados digitais para autenticação entre equipamentos utilizando criptografia de Estado.
          3. Deve suportar utilização de certificados digitais externos e internos gerados internamente na solução.
          4. A solução deve ter a capacidade de exportar requisições de certificados utilizando criptografia de Estado e aceitar certificados assinados por autoridades certificadoras externas ao equipamento.
      36. Hardware
          1. Gerenciamento de chaves com certificação FIPS 140-3 nível 3
          2. O elemento de rede proposto deve ter uma arquitetura separada de controle e plano de dados (serviço)
          3. O elemento de rede proposto deve ter a unidade de processamento principal redundante, a fonte de alimentação e o relógio.
          4. A unidade de processamento principal, a fonte de alimentação e a placa de interface do elemento de rede proposto devem ser hot swappable.
          5. Durante a permuta, a função hot swappable do elemento de rede proposto não deve causar qualquer perda de pacotes.
          6. Durante o funcionamento redundante, os módulos devem funcionar em modo de espera Active/Standby. Em caso de falha do módulo, a unidade redundante deve manter a operação do roteador sem interrupções, como roteamento, encaminhamento, etc. Durante o failover não deve haver perda de pacotes.
          7. Durante uma elevada carga do CPU, o elemento de rede proposto deve poder ser acedido sem qualquer degradação da interação.
          8. Durante a alta temperatura, o elemento de rede proposto deve poder proteger-se de danos. O Proponente deve indicar a temperatura máxima permitida e explicar a estratégia de contingência se o limite atingir (por exemplo, desligamento automático).
          9. A falha de um dos principais componentes não deve afetar a operação e a funcionalidade, sem intervenção manual.
          10. O elemento de rede proposto não deve ter um único ponto de falha que possa afetar as operações normais.
          11. Para comprovar essa alta disponibilidade, forneça um relatório de teste de terceiros.
          12. O elemento de rede proposto deve suportar uma arquitetura de hardware flexível e escalável, considerando para isso:

Escolha do tamanho do chassi, número de slots, capacidade de roteamento;

Utilização ideal do slot através do uso de óptica plug-gable (SFP) (qualquer interface, qualquer slot);

Proteção de investimento maximizada e longevidade dos ativos por meio de interfaces e portabilidade de módulos;

* + - * 1. O hardware do Encriptador deve resistir e reagir a invasão física de seu perímetro.
        2. Deverá possuir hardware dedicado para instalação de algoritmo critpgráfico de estado a ser desenvolvido e fornecido pelo governo brasileiro;
        3. O hardware dedicado a criptografia deverá possuir proteção contra leitura externa e modificação externa não autorizada;
        4. O hardware dedicado a criptografia deverá possuir gerador de números aleatórios baseados em efeitos físicos, aprovado por órgão de segurança;
        5. O solução deve possuir mecanismo de auto teste de funções criptográficas (BIST), executado a cada inicialização;
        6. Deve suportar a operação de mais de um algoritmo criptográfico simultaneamente;
        7. Deve suportar a utilização de certificados digitais em qualquer modo de tunelamento, com verificação de validade e revogação dos mesmos;
        8. Deve suportar tuneis IPSEC e SSL;
        9. Deve suportar IKEv2 para tuneis IPSEC;
        10. Geração de alarmes via traps SNMPv2 para o sistema de gerência.
        11. Geração de alarmes via traps SNMPv3 para o sistema de gerência.
        12. O fornecedor deve demonstrar que o equipamento ofertado foi concebido utilizando boas práticas de segurança de hardware em seu projeto.
        13. É necessário demonstrar o atendimento aos quesitos da norma FIPS-140-3, nível 3.
        14. É importante que não existam vulnerabilidades de hardware ou software, que afetem a segurança da informação e, caso sejam identificadas posteriormente, devem ser corrigidas pelo fabricante.
        15. A PROPONENTE deve informar quais certificações de segurança o hardware possui.
        16. A PROPONENTE deve informar se a atualização do firmware requer um binário cifrado?
        17. A PROPONENTE deve informar se o hardware aceita firmwares não assinados.
        18. A solução deve suportar atualização do firmware segura, ou seja, ser tolerante a interrupções no processo de atualização.
        19. As memórias dos dispositivos devem armazenar os firmwares cifrados.
        20. As comunicações entre os componentes devem ser cifradas.
        21. A PROPONENTE deve descrever a estratégia para mitigar ataque de injeção de falhas.
        22. A PROPONETNE deve descrever a estratégia para mitigar ataque de canal lateral.
        23. A PROPONENTE deve informar se o hardware é resiliente a interferências eletromagnéticas.
        24. O equipamento deve empregar uma bateria que seja capaz de manter o funcionamento da proteção anti-tampering e os dados sensíveis na ausência de alimentação elétrica.
        25. A PROPONENTE deve informar qual a duração esperada da carga da bateria.
        26. O sistema deve emitir alertas de nível baixo da carga das baterias.
        27. O sistema não deve ser afetado em função de uma eventual falha na bateria.
        28. A PROPONENTE deve informar se a substituição da bateria exige interrupção do sistema.
        29. Eventual falha no processo de troca das baterias não deve causar a perda das chaves.
        30. O equipamento deve possuir um perímetro criptográfico com segurança aumentada, onde os dados sensíveis são gerados e armazenados cifrados e que permita sua resinagem.
        31. A PROPONENTE deve descrever como implementa o perímetro criptográfico.
        32. A PROPONENTE deve informar se o perímetro criptográfico é ou pode ser resinado.
        33. A PROPONENTE deve informar se todas as comunicações externas ao equipamento são cifradas, destacando as possíveis exceções.
        34. O equipamento deve contemplar uma solução anti-tampering, que efetue o apagamento de todas as chaves e quaisquer outros dados sensíveis.
        35. O hardware deve possuir funcionalidades anti-tampering para detecção e reação à tentativa de intrusão física. A PROPONENTE deve descrever a estratégia adotada para esse tipo de ataque.
        36. O hardware deve possuir funcionalidades anti-tampering para detecção e reação à manipulação da fonte de energia. A PROPONENTE deve descrever a estratégia adotada para esse tipo de ataque.
        37. O hardware deve possuir funcionalidades anti-tampering para detecção e reação à manipulação de temperatura. A PROPONENTE deve descrever a estratégia adotada para esse tipo de ataque.
      1. INTERFACE
         1. A PROPONENTE deve descrever as portas disponíveis no equipamento ofertado, com relação à:

1. Quantidade e velocidade de interfaces elétricas (100/1000Mbps);
2. Quantidade e velocidade de interfaces ópticas (1/10/100Gbps);
3. Quantidade de interfaces monomodo e multimodo.
   * + - 1. Adicionalmente, cotados de forma opcional, a PROPONENTE poderá listar outras opções de modelos de equipamento, em caráter de LPU, com seus respectivos preços unitários, possibilitando a EAF comprar separadamente, adicionar, ou alterar os modelos oferecidos inicialmente na solução proposta pela PROPONENTE.
         2. Suporte a agregação de interface de rede;
         3. Suporte a Arquitetura Full Mesh;
         4. Interface de gerenciamento dedicada.
         5. Latência agregada não deve ser maior que 15 microsegundos
         6. Deverá suportar IPV4 e IPV6
         7. Deve suportar o diagnóstico básico de interfaces ethernet, com informações sobre line protocol, speed/duplex;
         8. Deve suportar a configuração de endereçamento IPv4, IPv6 e dual stack (IPv4 + IPv6) em interface ethernet LAN, WAN e Gerência;
         9. Deve suportar o diagnóstico básico de interfaces ethernet LAN, WAN e Gerência através de ICMP (ping / traceroute);
         10. Deve suportar jumbo frames com MTU mínimo de 9000 bytes nas interfaces LAN e WAN;
         11. Deve criptografar/descriptografar 1Gbps/10Gbps/100Gbps de pacotes ethernet/IP clear-text, sem perda de pacotes.
       1. Segurança
          1. O equipamento proposto deve suportar AAA com integração com RADIUS ou TACACS/+.
          2. O equipamento proposto deve ter a capacidade de recorrer à palavra-passe local no caso de os servidores TACACS+ não estarem disponíveis.
          3. O equipamento proposto deve suportar o registo de violações de acesso.
          4. O equipamento proposto deve suportar a função de níveis de acesso ou comando por ID de utilizador e palavra-passe.
          5. O equipamento proposto deve ter a capacidade de atribuir privilégios de comando por conta de utilizador individual.
          6. O equipamento proposto deve suportar um tempo limite de marcha lenta configurável para sessões de início de sessão.
          7. O equipamento proposto deve ter a capacidade de ver quem está logado.
          8. O equipamento proposto deve ter a capacidade de remover uma sessão TTY/VTY ativa no router.
          9. O equipamento proposto deve fornecer encriptações para todas as palavras-passe, chaves secretas e chaves SNMP.
          10. O equipamento proposto deve suportar o seguinte Transporte Seguro:
4. SSH v2;
5. Cliente e servidor SSH.
   * + - 1. O equipamento proposto deve suportar a ACL de taxa de linha para filtragem de pacotes e limitação de taxa com base nas informações das camadas 3 e 4 e na contabilidade de acertos.
         2. O elemento de rede proposto deve suportar o policiamento automático do plano de controlo para proteger automaticamente os recursos do plano de controlo contra ataques sem adição manual de ACLs/filtros.
         3. O equipamento proposto deve suportar a filtragem para o acesso administrativo de entrada (telnet/ssh).
         4. O equipamento proposto deve suportar a filtragem do endereço de origem IP para acesso SNMP restrito.
         5. O equipamento proposto deve apoiar a estatística de permissão ou negação.
         6. O desempenho de encaminhamento do equipamento proposto não deve degradar-se substancialmente com um grande número de ACLs/filtros ativos.
         7. O equipamento proposto deve suportar o Protocolo de Tempo de Rede.
         8. O elemento de rede proposto deve suportar o tráfego de difusão iniciado pelo utilizador com limite de taxa
       1. Comunicação Segura
          1. O elemento deve ser capaz de utilizar algoritmos customizados e propriatários para criptografia, como o Algoritmo de Estado Brasileiro.

# Licenciamento – Suporte e garantia do produto

* + - 1. A PROPONENTE deve fornecer o controle de descrição de licença de todos os elementos da solução.
      2. A PROPONENTE deve fornecer a descrição detalhada de todas as licenças e certificados integrados no sistema que são fornecidas pela própria, ou por terceiros.
      3. As licenças de uso de software, de usuários, ou de serviços deverão ser perpétuas, sem data para expirar.

# Políticas e alinhamentos de segurança da informação:

1. A solução deve atender às políticas e diretrizes de segurança da informação solicitadas pela EAF.
2. É essencial que as leis governamentais vigentes sobre segurança cibernética e proteção de dados do Brasil sejam cumpridas, bem como as leis da Agência Nacional de Telecomunicações do Brasil (ANATEL).
3. A PROPONENTE tem a obrigação de gerar um documento no qual seja estabelecido o devido cumprimento do regulamento, especificando como e de que forma cada artigo corresponde aos regulamentos das resoluções.

# Roadmap de Hardware e Software:

* + - 1. A PROPONENTE deverá fornecer Roadmap detalhado de hardware e software pelo menos para os próximos 3 anos.
      2. A PROPONENTE deve fornecer o ciclo de vida detalhado (hardware e software) do sistema (desde a disponibilidade geral (GA) até o fim da vida útil (EOL)).
      3. Todos os tipos de hardware devem ser da versão mais recente, não devem estar com término de comercialização (end-of-sale) anunciado (os produtos devem estar em produção e serem comercializados pelo fabricante no momento da assinatura do contrato) e ter, pelo menos, 5 anos antes do fim do suporte, contados a partir do tempo de contrato assinado.
      4. Durante o ciclo de vida do hardware, no caso de atualização de software que requeira adição/substituição de hardware, o fornecedor será responsável por fornecê-lo gratuitamente.
      5. Todas as versões de software devem ser a versão mais recente e ter pelo menos 3 anos antes do fim do suporte, além de suporte para desenvolver novos patchs de software de correção, contando a partir do tempo de contrato assinado.
      6. A PROPONENTE deve garantir que uma nova versão do software ou firmware contenha todas as funções das versões anteriores e que a introdução desta não prejudique a interoperabilidade da mesma na rede;
      7. Durante todo o período de garantia, a PROPONENTE deve substituir, recuperar e/ou modificar os softwares e firmwares instalados, sem ônus de qualquer natureza à CONTRATADA, nos casos comprovados de mau funcionamento, de modo a ajustá-los aos resultados que atendam às especificações técnicas solicitadas para a nova solução de telecomunicações, ou para a parte de gerência.
      8. Deve suportar a atualização de software, firmware, bitstream FPGA e algoritmos plugáveis de estado, localmente em campo e remotamente;

# Gerenciamento de Falhas (FM)

* + - 1. Gerenciamento de Falhas refere-se à detecção, isolamento e correção de uma falha ou condição anormal.
      2. A solução deve cumprir os requisitos Gerencialmento de Falhas definidos pela recomendação ITU-T M.3400, 3GPP TS 28.518 e os requisitos listados abaixo.
      3. Vigilância de alarmes: inclui coleta, manuseio, correlação e encaminhamento de alarmes.
      4. Localização de falhas: analisa as informações de alarme coletadas, detecta a causa raiz do alarme e notifica o resultado aos clientes do monitoramento de alarme.
      5. Correção de falhas: restaura e recupera o elemento de recurso de rede.
      6. Filtragem e gerenciamento de filtros: a interface do usuário deve permitir a filtragem e classificação de eventos por qualquer valor de campo de alarme.
      7. Teste: invoca uma capacidade de teste de um elemento de recurso mediante solicitação do cliente do serviço.
      8. Administração de falhas: permite o relatório de condições de falha e o rastreamento de seu status.
      9. O Fornecedor deve fornecer uma descrição completa de suas capacidades de Gerenciamento de Falhas.
      10. Deve suportar mecanismos de controle de acesso e criptografia de SNMPv3;
      11. Deve suportar SNMPv2 e SNMPv3;
      12. Deve suportar transporte SNMP em IPv4 / IPv6 / UDP;
      13. Deve implementar MIBs de interface ipv4, ipv6 e roteamento;
      14. Deve definir e implementar MIBs necessários relativos aos tunéis, algoritmos de criptografia, políticas de criptografia e também os modelos de status operacionais dos mesmos;
      15. Implementar RFC 2570, SNMP Version 3 Framework;
      16. Implementar RFC 2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3);
      17. Implementar RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP);
      18. Implementar RFC 2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP);
      19. Implementar RFC 3826, The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model;
      20. Implementar RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP);
      21. Implementar RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP);
      22. Implementar RFC 4293, Management Information Base for the Internet Protocol (IP);
      23. Implementar RFC2465, Management Information Base for IP Version 6;
      24. Implementar IANA address family numbers MIB;
      25. Implementar IANA ifType MIB;
      26. Implementar RFC 2578, Structure of Management Information Version 2 (SMIv2);
      27. Implementar a função da RFC 2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2;
      28. Implementar RFC 2012, SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2;
      29. Implementar RFC 2013, SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2;
      30. Implementar RFC 4292, IP Forwarding Table MIB;
      31. Implementar Interface Index (ifIndex) persistence;
      32. Implementar RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP) (SNMP over UDP over IPv4);
      33. Implementar RFC 2863, The Interfaces Group MIB;
      34. Implementar RFC 2571, An Architecture for Describing SNMP Management Frameworks;
      35. Implementar a função da RFC 4001, Textual Conventions for Internet Network Addresses;
      36. Implementar RFC 3164, The BSD syslog Protocol;
      37. Implementar Syslog local e remoto;
      38. Implementar múltiplos servidores Syslog remotos;
      39. A solução de gerência deverá ser centralizada para toda a solução, sem necessidade de subdivisões em função da quantidade de ativos;
      40. A gerência deve ser implantada com sua capacidade total de dimensionamento,, independentemente da quantidade de Encriptadores adquiridos/ativados, ou seja, a gerência deve considerar a solução completa desde o início do projeto.

# Gerenciamento de Configuração (CM)

* + - 1. Gerenciamento de Configuração envolve trabalho em dados de configuração associados ao elemento de rede gerenciado.

1. A solução deve cumprir os requisitos Gerenciamento de Configuração definidos pela recomendação ITU-T M.3400, 3GPP TS 28.510 e os requisitos listados abaixo.
2. Utilização de recursos: envolve a representação de dados sobre a eficácia da configuração em relação ao desempenho da rede.
3. Provisionamento de rede: envolve a configuração de elementos de rede para oferecer um serviço; rede é configurada usando interfaces interativas para operação adequada.
4. Descoberta automática: o processo em que o aplicativo de gerenciamento verifica e descobre recursos na rede. O estado do recurso (em serviço, offline, ocupado, etc.) e seus atributos devem ser exibidos e usados no aplicativo de gerenciamento.
5. Backup e recuperação automáticos: é fundamental fazer backup das informações de configuração e restaurar os dados quando necessário.
6. Gerenciamento de inventário: envolve o controle dos recursos (ativos e inativos) na rede para que possam ser alocados, provisionados, implementados ou mantidos como backup. A saída da descoberta automática é alimentar o gerenciamento de inventário para sincronizar o status dos recursos que estão alocados na rede a qualquer momento
7. Gerenciamento de mudanças: a mudança de status dos elementos de rede precisa ser continuamente monitorada e atualizada.
8. Pré-provisionamento: um conjunto de parâmetros precisa ser definido durante o provisionamento. A decisão efetiva sobre os parâmetros a serem definidos pode ser obtida pela análise de tendência do elemento de rede. Isso ajuda a determinar os parâmetros de provisionamento e, portanto, faz parte do processo de pré-provisionamento.
9. O Fornecedor deve fornecer uma descrição completa de suas capacidades Gerenciamento de Configuração.
10. Deve possuir interfaces CLI com acesso local via interface ethernet de gerência ou interface serial, e NETCONF/YANG, Web e SNMPv3 para gerenciamento remoto;
11. O gerenciamento remoto deverá ser feito através de endereçamento IPv4 ou IPv6, em interface ethernet dedicada de gerência, ou interface WAN/LAN, ou em subinterface vlan;
12. Deve suportar a configuração de interfaces ethernet WAN, LAN e Gerência, incluindo endereçamento IPv4 / IPv6, vrf, speed/duplex e vizualização da configuração e status operacional;
13. Todas as interfaces de gerenciamento (CLI Local / Remoto, NETCONF/YANG, WEB, SNMPv3) devem exigir autenticação. O gerenciamento remoto somente poderá ser realizado através de transporte criptografado (SSL/TLS, SSH, IPSEC);
14. Deve suportar a gestão de chaves públicas e privadas e certificados;
15. Deve suportar a gestão de tuneis criptográficos, visualização de sua configuração e status operacional;
16. Deve suportar a criação e gestão de usuários / grupos / privilégios de acesso para AAA CLI, SNMPv3 e TACACS;
17. Deverá suportar TACACS+;
18. A interface CLI deverá ser acessível também via SSH;
19. Deve possuir base local para controle de usuários, grupos e permissões;
20. Deve possuir interface Web https permitindo executar pelo menos as mesmas configurações obrigatórias da interface CLI;
21. Deve suportar a configuração em massa de equipamentos, inclusive com o recurso de embarque de algoritmo de Estado.
22. Deverá suportar Secure Zero Touch Provisioning (SZTP);
23. Implementar a função da RFC 1492 TACACS+;
24. Implementar a função do draft-grant-tacacs-02, The TACACS+ Protocol;
25. Implementar autenticação mútua entre o servidor AAA e o cliente AAA;
26. Implementar definição de grupos de usuários, com diferentes níveis de acesso;
27. Implementar RFC 4250, The Secure Shell (SSH) Protocol Assigned Numbers;
28. Implementar RFC 4251, The Secure Shell (SSH) Protocol Architecture;
29. Implementar RFC 4252, The Secure Shell (SSH) Authentication Protocol (public key, password;
30. Implementar RFC 4253, The Secure Shell (SSH) Transport Layer Protocol;
31. Implementar RFC 4254, The Secure Shell (SSH) Connection Protocol;
32. Implementar RFC 5905 NTP, incluindo autenticação;
33. Implementar RFC 8572, Secure Zero Touch Provisioning (SZTP), incluindo as capacidades 4.1, 4.2, 4.3, 4.4 e o modelo de dados 6.1;
34. Implementar RFC 6020, YANG - A Data Modeling Language for NETCONF;
35. Implementar RFC 6241, NETCONF - Network Configuration Protocol, incluindo as capacidades 8.3, 8.4, 8.5 e 8.6;
36. Implementar RFC 6242, Using the NETCONF Protocol over Secure Shell – SSH;
37. Implementar RFC 7589, Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication;
38. Implementar RFC 7923, Requirements for Subscription to YANG Datastores;
39. Implementar RFC 5277, NETCONF Event Notifications;
40. Implementar os modelos YANG: RFC8177, YANG Data Model for Key Chains, draft-ietf-netconf-crypto-types-14;
41. Implementar os modelos YANG opencofig (https://www.openconfig.net/projects/models/): acl, aft, interfaces, local-routing, network-instance, platform, policy-forwarding, system, vlan.
42. A solução de gerência deverá ser centralizada para toda asolução, sem necessidade de subdivisões em função da quantidade de ativos;
43. A gerência deve ser implantada com sua capacidade total de dimensionamento,, independentemente da quantidade de Encriptadores adquiridos/ativados, ou seja, a gerência deve considerar a solução completa desde o início do projeto.

# Gerenciamento de Performance (PM)

* + - 1. O Gerenciamento de Performance envolve a avaliação e o relatório do comportamento e eficácia dos elementos da rede, reunindo informações estatísticas, mantendo registros históricos, determinando o desempenho do sistema e alterando os modos de operação do sistema.

1. A Solução deve cumprir os requisitos de PM definidos pela recomendação ITU-T M.3400, 3GPP TS 28.523 e os requisitos listados abaixo:
2. Coleta de dados de desempenho: para cada elemento da rede, há um conjunto de indicadores-chave de desempenho (KPIs). A coleta de dados relacionados a esses KPIs ajuda a determinar e prever a integridade da rede.
3. Utilização e taxas de erro: Ao avaliar casos de tendências de utilização abaixo e acima, limites e taxas de erro garantem a utilização ideal dos recursos de rede.
4. Disponibilidade e desempenho consistente: a verificação mais básica de desempenho é a disponibilidade de um recurso.
5. Análise de dados de desempenho e geração de relatórios: todos os aplicativos de gerenciamento de desempenho têm a capacidade de coleta de dados, análise de dados e geração de relatórios. Vários relatórios podem ser gerados como gráficos e plotagens dos dados de desempenho. A análise de dados também envolve a criação de correlações e a descoberta de resultados correlacionados nos dados de limite. A exportação de dados para análise por aplicativos de terceiros também deve ser suportada.
6. Planejamento de estoque e capacidade: os dados de desempenho são usados como entrada para planejamento de estoque e intervenções de planejamento de capacidade.
7. O Fornecedor deve fornecer uma descrição completa de suas capacidades de Gerenciamento de Performance.
8. Deve suportar a visualização de logs e traces de troubleshooting e debug, em particular os relacionados ao estabelecimento e situação operacional de túneis.
9. A PROPONENTE deve informar qual a taxa mínima e máxima de transferência atingida pela solução, considerando na resposta as condições de teste, perda de pacotes, duração do teste, renegociações de chaves e tráfego simulado.
10. A solução de gerência deverá ser centralizada para toda asolução, sem necessidade de subdivisões em função da quantidade de ativos;
11. A gerência deve ser implantada com sua capacidade total de dimensionamento,, independentemente da quantidade de Encriptadores adquiridos/ativados, ou seja, a gerência deve considerar a solução completa desde o início do projeto.

# Certificado de conformidade

* + - 1. A PROPONENTE deve garantir, junto à autoridade reguladora (ANATEL), que o equipamento oferecido seja certificado e aprovado para implantação e operação no Brasil.
      2. Esse Certificado de Homologação deverá ser apresentado no envio da PROPOSTA Técnica/Comercial.
      3. Todos os custos associados à homologação são por conta da PROPONENTE.
      4. O equipamento deve ser etiquetado de acordo com os requisitos regulamentares do Brasil.

# Sobressalentes

* + - 1. A PROPONENTE deverá disponibilizar peças sobressalentes para o sistema na ativação comercial. As peças sobressalentes devem representar pelo menos 5% do valor total do hardware do sistema.
      2. Após o término da garantia, a Proponente deverá fornecer sobressalentes que sejam compatíveis em forma, montagem e funcionamento pelo prazo de 02 (anos).
      3. O preço das peças sobressalentes deverá ser cotado unitariamente em LPU, conforme o ”**03\_Anexo\_C–LPU-Proposta\_Comercial\_Encriptadores**”.
      4. Se após o período de 05 (cinco) anos a Proponente tender a descontinuar a fabricação de quaisquer partes dos suprimentos objeto deste contrato, a Proponente deverá notificar a Compradora com pelo menos 01 ano de antecedência dessa descontinuação. A PROPONENTE deverá oferecer ao COMPRADOR a oportunidade de solicitar, a um preço razoável, as quantidades de peças de reposição que o COMPRADOR possa razoavelmente exigir em relação à vida útil prevista dos suprimentos.

# Requisitos de Manutenção e Suporte Operacional

* + - 1. A PROPONENTE deverá estabelecer contato com a equipe de Operação e Manutenção da EAF e prover atualizações sobre os problemas relacionados ao Hardware/Software que possam ser gerados e/ou resolvidos em qualquer outro mercado/operação, em periodicidade mensal;
      2. A escalação ao Terceiro Nível de suporte será gerenciada pelos termos do Acordo de Nível de Serviço (SLAs), sendo gerenciada pelos representantes responsáveis da equipe de Operação e Manunteção da EAF de nível 2 (L2), onde a empresa fornecedora precisa estar em cooperação total com nossos representantes de Operação e Manutenção;
      3. Após restaurações de falhas, o suporte nível 3 (L3) deverá enviar um relatório por escrito contendo a descrição detalhada dos problemas, com recomendações de ações para mitigação e resolução, as quais deverão ser revisadas e acompanhadas em reuniões regulares com a operadora e os representantes da equipe de Opedração e Manutenção da EAF;
      4. Com o objetivo de apoiar a EAF na operação da rede, a PROPONENTE deverá oferecer serviço de Operação Assistida no período de 12 meses em regime de 8x5;
      5. Para o serviço de Operação Assistida, a PROPONENTE deverá manter localmente (on-site), no mínimo, 1 (um) recurso, além dos recursos que ficarão disponíveis remotamente.
      6. A emissão do Termo de Aceitação Definitiva, ou a entrada da Solução em Operação Comercial, marca o início dos serviços de Operação Assistida.

# Desenvolvimento de Competências e Transferência de Conhecimento

* + - 1. A PROPONENTE deverá executar o desenvolvimento de competências e serviços de transferência de conhecimento para viabilizar à EAF a construção de competência técnica e conhecimento a todos os recursos existentes de operações/otimização e Serviços Gerenciados, aumentando assim, a eficiência e qualidade dos serviços entregues, satisfação do usuário final e redução de custos, garantindo a confiabilidade, segurança e a informação atualizada durante o contrato;
      2. A PROPONENTE deverá disponibilizar informações corretas no tempo adequado às Equipes do Cliente e Serviços Gerenciados que requeiram tais informações, a fim de possibilitar ao Cliente a correta tomada de decisões. As responsabilidades da PROPONENTE dos serviços de gerenciamento de conhecimento deverão incluir:

1. Atualização de banco de dados de conhecimento contendo todos os eventos, incidentes e problemas, com a revisão do conteúdo em periodicidade semanal;
2. Acesso completo aos especialistas da PROPONENTE e ao sistema de treinamentos/transferência de conhecimento pelas equipes da EAF e de Serviços Gerenciados;
3. Treinamentos adequados ao uso do banco de dados de conhecimento às equipes da EAF e Serviços Gerenciados;
4. Plano completo de treinamentos, desenvolvimento de competências e transferência de conhecimento com pontos de controle (“milestones”) claramente definidos, Estrutura Analítica de Projetos (EAP) - conhecida também como WBS, tópicos de treinamento e desenvolvimento, pré-requisitos, entregáveis esperados, prazos, relatando periodicamente o andamento da implementação deste plano à EAF;
   * + 1. A PROPONENTE proverá treinamentos e o desenvolvimento contínuo de transferência de competências às equipes da EAF e Serviços Gerenciados sempre e quando necessário, incluindo treinamentos de produtos e plataformas da empresa fornecedora, suporte à operação e manutenção e otimização de performance de todos os equipamentos da PROPONENTE e todo e qualquer produto de terceiros se houver, incluindo e não limitado a:
5. Gerenciamento de Falhas;
6. Configuração de Sistema;
7. Gerenciamento de Mudanças;
8. Gerenciamento de Performance;
9. Vigilância e monitoração da rede e performance;
10. Gerenciamento de Problemas;
11. Atualizações e upgrades de software e implementações de FNI;
12. Aceitação de novos elementos de rede e comissionamento;
13. Conceitos básicos sobre expansão de hardware e software da solução;
14. Upgrades de hardware;
15. Monitoração de performance de rede e otimização;
16. Integração de rede, rollout e serviços de implantação;
17. Implementação de algoritmo de criptografia customizado (ex: algoritmo do Estado);
    * + 1. O escopo de tais treinamentos e a transferência de competências devem incluir as equipes da EAF e de Serviços Gerenciados responsáveis pela operação e manutenção e otimização dos sistemas disponibilizados pela PROPONENTE.
        2. A PROPONENTE deve oferecer treinamentos (presenciais, ou remotos) que possibilitem a EAF a operar o sistema;
        3. A PROPONENTE deve disponibilizar as ementas dos respectivos treinamentos;
        4. A PROPONENTE não fará alterações de atualizações tecnológicas nos equipamentos, e/ou software, e/ou mudanças nos serviços suportados, a menos que as equipes da EAF e de Serviços Gerenciados tenham recebido treinamento com antecedência nos novos equipamentos, e/ou software, e/ou serviços de suporte relacionados;
        5. A PROPONENTE prontamente notificará a EAF de quaisquer requisitos de treinamento, para assegurar a certificação.

# Embarque de Algoritmo de Criptografia do Estado Brasileiro

* + - 1. A solução deve possuir uma ferramenta centralizada que permita atualização remota de firmware;
      2. Deve ser disponibilizada amostra mínima de equipamentos para que órgão de segurança do governo realize testes de homologação e embarque inicial do algoritmo.
      3. Os códigos fonte dos dispositivos onde forem implementados o algoritmo de estado devem ser disponibilizados para órgão de segurança do governo.
      4. O processo de homologação, incluindo testes de embarque do algoritmo de Estado, poderá ser efetuado durante PoC (Proof of Concept) a ser realizado antes da adjudicação.
      5. Procedimento sugerido para o embarque do algoritmo de Estado:
         1. O encriptador possui firmware com chave pública pré-gravada a fim de autorizar instalações apenas de firmwares assinados com a chave privada correspondente;
         2. Para embarcar o Algoritmo do Estado, deverá ser utilizada uma versão intermediária de firmware com nova chave pública, correspondente a uma chave privada gerada e armazenada por órgão do governo;
         3. O firmware intermediário é assinado pelo PROPONENTE, de forma que apenas firmwares assinados com a chave de governo sejam aceitos nos encriptadores;
         4. Todos os dispositivos são atualizados remotamente com o firmware intermediário;
         5. A partir de então, todo firmware só é atualizado se estiver assinado pelo órgão de segurança do governo.
         6. Abaixo figura esquema simplificado do processo de atualização:

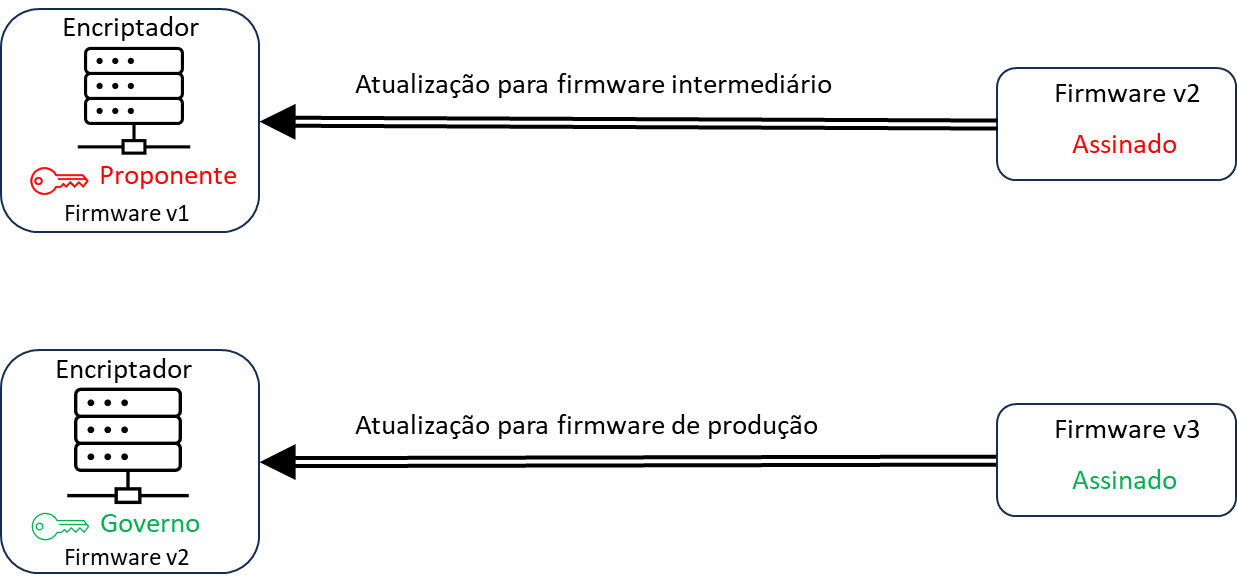


Figura 9 – Atualização de firmware num único Encriptador

# Serviços

# Projeto

* + 1. Validação do modelo de tráfego e dimensionamento da solução.
    2. Site Survey – avaliação do local físico onde serão instalados os equipamentos, para verificações de questões relacionadas à localização de bastidores, energização, aterramento, caminho de fibras, calhas, esteiras, pontos de conexão com a rede da EAF, etc;
    3. Elaboração de Relatório PPI (Projeto Provisório de Instalação) fotográfico e com as informações do site, para validação da EAF;
    4. Após o aceite da instalação pela EAF, a PROPONENTE deverá elaborar/atualizar o Relatório emitindo o PDI (Projeto Definitivo de Instalação);
    5. A PROPONENTE deverá fornecer documentação completa do projeto com HLD (High Level Design) e LLD (Low Level Design), incluindo nesses documentos, a descrição detalhada de toda a solução.
    6. A PROPONENTE deverá disponibilizar Projeto Executivo, HLD e LLD por cliente a ser atendido pela solução;
    7. O cronograma deve contar com a fase inicial de investigação de serviço, onde serão definidas as informações que serão utilizadas no projeto.

# Entrega de Equipamentos

* + 1. É de responsabilidade da PROPONENTE a entrega, recebimento, conferência e acomodação de todos os materiais e equipamentos desta contratação;
    2. A entrega de cada equipamento deverá ser realizada no destino final de instalação;
    3. Entre a fase de recebimento do material e entrega definitiva em campo pela PROPONENTE, o armazenamento deverá ser feito em Warehouse da própria PROPONENTE, sem custos para a CONTRATANTE.

# Instalação;

* + 1. Instalação de todos os elementos de rede nos gabinetes/bastidores;
    2. Energização dos equipamentos, de acordo com o projeto e com as posições de PDU/Disjuntores que forem verificadas e aprovadas na vistoria de implantação (Site Survey);
    3. Passagem de cabos e fibras ópticas, de acordo com o projeto e com o que for aprovado na vistoria de implantação (Site Survey);
    4. As fibras ópticas fornecidas pela PROPONENTE devem ser MONOMODO ou MULTIMODO. Essa definição se dará em tempo de projeto, de acordo com o que for aprovado pela EAF na análise do relatório de Site Survey;
    5. Todos os cabos e fibras devem ser devidamente identificados de acordo com a padronização a ser definida na fase de Service Investigation;
    6. A PROPONENTE deverá fornecer e instalar todos os materiais necessários para a conexão óptica/elétrica e cabos de energia para energização dos equipamentos incluindo as conexões com outros equipamentos existentes, e com elementos de Acesso Remoto a Console (gerência out-of-band), etc., em qualquer horário e qualquer dia de semana. Deverão ser consideradas todas as conexões definidas na Topologia do projeto.
    7. Todos os materiais necessários para a completa instalação dos equipamentos deste projeto deverão ser fornecidos (conectores, cabos de energia e sinal, identificações, , kits de fixação, etc.).
    8. A PROPONENTE deverá providenciar a retirada do local de sobra de material de instalação, responsabilizando-se pela destinação adequada dos resíduos gerados.

# Comissionamento, Integração e Testes

* + 1. Comissionamento de todos os elementos da solução;
    2. Integração de todos os elementos da solução internamente, e com elementos externos (LAN, BBIP, Roteadores, Switches, SD-WAN, Gerência, Alarmística, etc...) a fim de deixar a solução pronta para os testes fim a fim;
    3. A PROPONENTE deve realizar testes de conectividade em todas as integrações necessárias para o correto funcionamento da Solução;
    4. A PROPONENTE deve realizar testes de funcionalidade (fim a fim) para validação da Solução;
    5. A PROPONENTE deve apoiar a EAF nos testes de aceitação da Solução;
    6. O caderno de testes de aceitação deve ser construído em comum entre PROPONENTE e EAF;
    7. Os testes de aceitação devem contemplar a validação do carregamento e uso do Algorítimo de Criptografia de Estado Brasileiro, verificando inclusive, a performance do equipamento com o esse algorítmo.

# Aceitação

* + 1. Devem ser realizados Testes de Aceitação em conjunto (PROPONENTE e EAF) a fim de garantir o correto funcionamento da solução;
    2. Em relação à parte física, a PROPONENTE deverá comprovar a conformidade com o que foi aprovado no relatório de Site Survey e com o Projeto Técnico;
    3. Em relação à parte lógica, a PROPONENTE deverá comprovar a conformidade com relatório comprobatório de testes;
    4. A EAF emitirá Termos de Aceitação Provisória (TAP), caracterizando o início do Período de Funcionamento Experimental (PFE);
    5. O TAP será emitido ao término dos Testes de Aceitação, se não houver pendências nos serviços executados, ou se a natureza das mesmas não impedir a ativação experimental dos equipamentos e/ou sistemas, ou não comprometer o desempenho e a segurança operacional, bem como as atividades de O&M. Este documento deverá ainda relacionar as eventuais pendências não impeditivas citadas;
    6. O Período de Funcionamento Experimental (PFE), iniciado na data de emissão do Termo de Aceitação Provisória, visa a medição da confiabilidade e/ou desempenho dos equipamentos, serviços e/ou sistemas, com duração de 30 (trinta) dias, após o qual a EAF poderá emitir o Termo de Aceitação Definitiva;
    7. Durante o Período de Funcionamento Experimental os equipamentos poderão ou não ser colocados em Operação Comercial, a critério da EAF;
    8. Durante o PFE poderão ser levantadas novas pendências, não incluídas inicialmente no TAP, as quais deverão ser eliminadas pela PROPONENTE até o término do PFE, ou, em casos de baixa criticidade, acordado um compromisso de data para a resolução entre PROPONENTE e EAF através de Termo de Compromisso;
    9. No caso do surgimento de falhas que comprometam o desempenho e/ou a segurança operacional dos equipamentos e/ou sistemas, o PFE deverá ser reinicializado após a remoção das mesmas;
    10. Durante o Período de Funcionamento Experimental, contado a partir da emissão do TAP a PROPONENTE colocará à disposição da EAF, técnicos para a operação e manutenção dos equipamentos, sem ônus para a mesma;
    11. Ao término do Período de Funcionamento Experimental, desde que não haja pendências de qualquer natureza, a EAF emitirá TERMO DE ACEITAÇÃO DEFINITIVA (TAD);
    12. A emissão do TAD, ou a entrada da Solução em Operação Comercial, marca o início dos serviços de suporte técnico e Operação Assistida.

# Gerência de Projeto

* + 1. A Gerência do Projeto deverá seguir as melhores práticas de gerenciamento de projetos do mercado;
    2. A metodologia deverá utilizar ferramentas e padrões baseados no PMI – Project Management Institute, permitindo-se adaptações em comum acordo entre PROPONENTE e EAF;
    3. A PROPONENTE será responsável por realizar o planejamento do projeto, junto à EAF, e garantir um andamento adequado do projeto com relação às metas e objetivos planejados, gerenciando riscos, tomando ações preventivas e corretivas sobre o projeto;
    4. O gerenciamento de projetos da PROPONENTE deve coordenar a prestação dos serviços no projeto e interagir constantemente com a EAF, posicionando-o sobre o andamento do projeto.