

DIRETORIA DE COMUNI E TEC. DA INF. DA MARINHA

Estudo Técnico Preliminar 90/2025**1. Informações Básicas**

Número do processo: 63394.000905/2025-80

2. Descrição da necessidade

A presente contratação tem por finalidade a renovação das licenças de atualização, suporte e garantia de dois equipamentos que integram a solução de segurança de borda da Rede de Comunicações Integrada da Marinha (RECIM). A manutenção dessas licenças é necessária para preservar a capacidade de proteção cibernética da infraestrutura de TIC da Marinha do Brasil, permitindo a continuidade das atualizações de segurança, do suporte técnico e da garantia dos equipamentos atualmente em uso.

A solução de segurança de borda composta pelos equipamentos firewall e Intrusion Prevention System (IPS) exerce papel essencial na mitigação de ameaças cibernéticas, na proteção dos sistemas, serviços e sítios institucionais, bem como na preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações trafegadas na RECIM. A ausência de licenciamento ativo comprometeria a capacidade de atualização, suporte e resposta a incidentes, elevando o risco de indisponibilidade, exploração de vulnerabilidades e degradação da segurança do ambiente tecnológico.

A partir de 2020, a Marinha do Brasil realizou investimento relevante na substituição dos equipamentos firewall e IPS, bem como na aquisição de suas respectivas licenças. Dessa forma, a renovação das licenças atualmente necessárias preserva o investimento já realizado, evita substituição prematura de ativos em operação, mantém a compatibilidade com o parque tecnológico existente e reduz riscos operacionais decorrentes de eventual descontinuidade de suporte ou de atualização de assinaturas de segurança.

O quantitativo foi revisto em razão da necessidade de manter plenamente funcional o parque tecnológico existente, considerando a ampliação das atividades de proteção cibernética da rede, a continuidade dos serviços institucionais suportados pela RECIM e o fato de que licenças anteriormente ativas expiraram em razão do lapso temporal decorrido durante a instrução processual. Assim, a quantidade inicialmente estimada tornou-se insuficiente, sendo necessário o ajuste do quantitativo para garantir a manutenção das soluções de segurança de borda em condições adequadas de operação, suporte e atualização.

2.1. Enquadramento como serviço comum

Os serviços objeto deste Estudo Técnico Preliminar são considerados comuns, nos termos do inciso XIII do art. 6º da Lei nº 14.133/2021, por apresentarem padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

No presente caso, a contratação abrange licenciamento, atualização, suporte e garantia de soluções de segurança cibernética em uso pela Administração, cujas características técnicas, condições de execução e critérios de desempenho podem ser descritos de forma clara, objetiva, padronizada e comparável entre os potenciais licitantes, permitindo julgamento objetivo das propostas.

A eventual complexidade tecnológica da solução não afasta seu enquadramento como serviço comum, uma vez que o elemento determinante é a possibilidade de definição objetiva do objeto e o domínio do mercado acerca de sua oferta e execução. Assim, a contratação é compatível com a adoção da modalidade pregão, na forma eletrônica, observadas as demais condições estabelecidas nos artefatos da contratação.

2.2. Alinhamento ao planejamento institucional

2.2.1. A presente contratação encontra-se alinhada aos instrumentos de planejamento institucional aplicáveis, em especial ao Plano de Contratações Anual/PAC, ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) vigente da DCTIM e aos objetivos estratégicos relacionados à segurança da informação, continuidade dos serviços de TIC, disponibilidade dos serviços digitais e proteção da infraestrutura crítica de comunicações da Marinha do Brasil.

2.2.2. No Plano de Contratações Anual/PAC, a demanda está relacionada aos itens de planejamento referentes à aquisição/renovação de serviços de atualização, suporte e garantia dos equipamentos de segurança de borda, especialmente aqueles relativos ao suporte dos equipamentos Firewall Cisco FPR2140 e IPS Trellix NS9500, conforme registros constantes dos autos.

2.2.3. A contratação também está alinhada ao PDTIC vigente, por contribuir diretamente para a manutenção do licenciamento de suporte necessário, para a continuidade operacional das soluções de segurança cibernética e para o fortalecimento da Segurança da Informação e das Comunicações, mediante preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações trafegadas na RECIM.

2.2.4. Quanto à Política de Governança Digital e à Plataforma gov.br, registra-se que o objeto não envolve desenvolvimento, implantação ou integração direta de serviço público digital ao cidadão na Plataforma gov.br. Trata-se de contratação de licenças, subscrições, atualização, suporte e garantia de soluções de segurança de borda já implantadas. Ainda assim, a contratação contribui indiretamente para a continuidade, disponibilidade e segurança dos serviços digitais institucionais mantidos pela Marinha do Brasil, ao preservar a capacidade de inspeção, prevenção, bloqueio e resposta a ameaças cibernéticas.

3. Área requisitante

Área Requisitante	Responsável
Divisão de Proteção Cibernética	Allan Rodrigo de Souza Braga

4. Necessidades de Negócio

- 4.1. Manter o parque tecnológico referente à solução Trellix Network Security Platform – Intrusion Prevention System (IPS) e Firepower, na Marinha do Brasil (MB) em plena operação, com as devidas atualizações de segurança e suporte remoto.
- 4.2. Manter e elevar o nível de qualidade e segurança dos serviços internos e externos disponibilizados por esta instituição.
- 4.3. Melhorar a granularidade de informações para resolução de incidentes de rede, com a utilização de ferramentas atualizadas.
- 4.4. Preservação da integridade e confidencialidade das comunicações entre a instituição e demais órgãos, quando se tratar de tráfego sensível.
- 4.5. Proteção da infraestrutura de TI desta instituição de modo a impedir que a mesma seja utilizada para outros fins (por exemplo: processamento no Datacenter utilizado para mineração de bitcoins, links de Internet utilizados para download de conteúdo ilícito ou ataques de negação de serviço – DDoS).
- 4.6. Prover comunicação segura entre as organizações desta instituição.
- 4.7. Manter a plataforma de tecnologia de segurança da informação utilizada por esta instituição.
- 4.8. A aquisição de licenças não poderá incorrer em investimentos adicionais de compra de ativos de hardware.
- 4.9. A aquisição de licenças não poderá incorrer em alteração de topologia ou de configurações e políticas já estabelecidas e configuradas no Sistema IPS atualmente em uso.
- 4.10. As licenças de software deverão ser compatíveis com o ecossistema do Sistema IPS do modelo 9500 e Firepower modelo 2140, atualmente adotado na Marinha do Brasil.

5. Necessidades Tecnológicas

- 5.1. Permitir análise de pontos fracos da rede, correlacionar eventos de ameaças automaticamente a vulnerabilidades da rede.
- 5.2. Proteção do ambiente de rede contra ameaças através da detecção e proteção em tempo real contra ameaças.
- 5.3. Permitir alta disponibilidade.
- 5.4. Permitir atualização contínua dos sistemas operacionais atuantes nos equipamentos principais da borda, seja o IPS ou o Firewall.
- 5.5. Permitir o pronto reparo e/ou substituição do equipamento do IPS modelo 9500, em caso de defeito.
- 5.6. Geração de informações diversas sobre tráfego, ameaças, entre outras, em tempo real para rápida análise.
- 5.7. Criação de políticas e medidas de segurança para proteção da rede contra tentativas de ataques e invasões.
- 5.8. A manutenção e atualização das licenças dos equipamentos firewall 2140 visam permitir que as seguintes necessidades sejam alcançadas:
 - 5.8.1. Permitir a criptografia do tráfego SSL para inspeção de conteúdo;
 - 5.8.2. Permitir inspeção em camada 7 (nível de aplicação);
 - 5.8.3. Permitir inspeção de conteúdo com capacidade de identificar e bloquear vulnerabilidades, vírus, *malwares* conhecidos e desconhecidos;
 - 5.8.4. Permitir a criação de redes seguras (VPN) de forma simples para que os usuários e os administradores possam utilizar a infraestrutura remotamente;
 - 5.8.5. Permitir a criação de redes seguras (VPN) entre a MB e outras instituições que demandam trafegar dados sensíveis;
 - 5.8.6. Implementar solução AMP (Advanced Malware Protection, proteção avançada contra malware) integrada que trate ameaças conhecidas e desconhecidas com um sandbox integrado; e
 - 5.8.7. Implementar solução de filtro de conteúdo e de URL, possibilitando a criação de regras de acesso a domínios na internet.

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

6.1. Requisitos Legais

- 6.1.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94/2022, à Instrução Normativa SEGES/ME nº 65/2021, à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), à Lei nº 12.965/2014 (Marco Civil da Internet), bem como às demais normas aplicáveis às contratações públicas de soluções de TIC.
- 6.1.2. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante.
- 6.1.3. A manutenção da padronização da solução cibernética de IPS e firewall corporativo está alinhada ao previsto no inciso V, alínea a, do art. 40 da Lei nº 14.133/2021.
- 6.1.4. Deverão ser cumpridas, no que couber, as exigências:
 - 6.1.4.1. Do inciso XI, art. 7º da Lei 12.305, de 02 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos — PNRS;
 - 6.1.4.2. Do art. 6º da Instrução Normativa MPOG nº 01, de 19 de janeiro de 2010, que estabelece as práticas de sustentabilidade na execução dos serviços; e
 - 6.1.4.3. Da Portaria Nº 170, de 10 de abril de 2012 do Instituto Nacional de Metrologia, Qualidade e Tecnologia — INMETRO.

6.2. Requisitos de Manutenção

- 6.2.1. Todos os prazos serão considerados após a abertura do chamado técnico na central de suporte da fabricante.
- 6.2.2. Manutenção preventiva
 - 6.2.2.1. Durante o prazo de garantia, deverá ser possível realizar a atualização de sistema operacional dos equipamentos, a fim de obter novas funcionalidades e correções. Durante o prazo de garantia, também deverá ser possível realizar a atualização das assinaturas de proteção da solução.

6.3. Manutenção corretiva

6.3.1 Durante o prazo de garantia, deverá estar prevista a reposição de peças e equipamentos. Essa reposição deverá abranger todos os itens que compõem a solução, incluindo módulos ou outros equipamentos fornecidos pela CONTRATADA para atendimento do edital.

6.3.2. Em caso de defeitos de fabricação ou necessidade de substituição de hardware, a garantia deverá incluir envio de peças ou equipamentos de reposição à CONTRATANTE.

6.3.3. O serviço de reposição de peças compreende o envio de materiais sobressalentes por parte do fabricante às dependências da CONTRATANTE em substituição a equipamento, componente, acessório ou dispositivo defeituoso coberto por este contrato de serviços e conforme comprovação do Centro de Assistência Técnica do fabricante no atendimento do chamado originário.

6.3.4. Após aberta a solicitação de substituição de peças (RMA) pelo Centro de Assistência Técnica do fabricante, inicia-se o prazo de fornecimento das peças substitutas, que será de até 30 dias úteis.

6.3.5. Deverá ser fornecido à CONTRATANTE, no momento da entrega do equipamento substituto e confirmação de seu recebimento, instruções para devolução sem ônus do equipamento substituído ao fabricante, em prazo máximo de dez dias úteis.

6.4. Suporte e comunicação

6.4.1. Durante o prazo de garantia, os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800), on-line no website do fabricante ou e-mail. O suporte deverá estar disponível na modalidade de 24x7 (24 horas por dia, 7 dias por semana).

6.4.2. Todos os prazos serão considerados após a abertura do chamado técnico na central de suporte da fabricante.

6.4.3. A Central de Suporte da fabricante deverá registrar a solicitação, gerando algum número, código ou protocolo que servirá de referência para acompanhamento.

6.5. Requisitos Temporais

6.5.1. Na contagem dos prazos estabelecidos no Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

6.5.2. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

6.5.3. A CONTRATADA deverá manter a capacidade de suporte e manutenção pelo período de vigência do contrato.

6.6. Requisitos de Segurança e Privacidade

6.6.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato.

6.6.2. A CONTRATADA deverá adotar todas as medidas necessárias para garantir que seus funcionários, representantes e/ou contratados sigam os regulamentos, normas e diretrizes de segurança da informação e Comunicações da MB, enquanto estiverem prestando serviços para a instituição.

6.6.3. A CONTRATADA deverá prestar os esclarecimentos necessários à MB, bem como informações concernentes à natureza e ao andamento dos serviços executados ou em execução.

6.6.4. A CONTRATADA deve se comprometer a manter em absoluto sigilo todas as informações confidenciais fornecidas pela MB, incluindo dados, configurações, processos, fórmulas, rotinas e qualquer outro material necessário para a execução dos trabalhos. Compromete-se a não copiar, utilizar em benefício próprio, divulgar ou compartilhar tais informações com terceiros, tanto no Brasil quanto no exterior, sob as penalidades previstas em lei. Somente os representantes e prepostos devidamente autorizados por ambas as partes, cuja análise das informações confidenciais seja essencial e apropriada para os fins estabelecidos em contrato, terão acesso a elas.

6.6.5. A CONTRATADA deverá tomar todas as providências necessárias para garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e solicitações efetuadas.

6.6.6. A Solução oferecida pela CONTRATADA deverá incluir um plano de comunicação de incidentes, e a CONTRATADA deverá informar imediatamente à CONTRATANTE sobre qualquer incidente de segurança da informação ou a identificação de vulnerabilidades relacionadas ao objeto do contrato. Isso inclui eventos inesperados ou indesejados, bem como qualquer violação das normas de sigilo estabelecidas, resultante de ação ou omissão, independentemente de dolo, que comprometam a confidencialidade, disponibilidade, integridade ou autenticidade dos dados da CONTRATANTE.

6.7. Requisitos Sociais, Ambientais e Culturais

6.7.1. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais.

6.7.2. As funcionalidades da solução deverão ser exibidas nas consoles, preferencialmente em português, ou, alternativamente, em inglês.

6.7.3. A CONTRATADA, bem como seus funcionários e prestadores de serviço, deverão observar as disposições da Instrução Normativa SLTI nº 01, de 19 de janeiro de 2010, que estabelece critérios de sustentabilidade ambiental para a aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional, além de outras providências;

6.7.4. Quando aplicável, a CONTRATADA deverá priorizar o uso de tecnologias ambientalmente responsáveis, utilizando materiais e equipamentos recicláveis ou reutilizáveis, conforme orientações do Guia de Contratações Sustentáveis, disponível no site da Advocacia-Geral da União (AGU).

6.8. Requisitos da Arquitetura Tecnológica

6.8.1. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

6.8.2. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

6.9. Requisitos de Experiência Profissional

6.9.1. Os serviços de suporte deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

6.10. Requisitos de Metodologia de Trabalho

6.10.1. A execução dos serviços está condicionada ao recebimento, pelo Contratado, da Nota de Empenho (NE) e do contrato emitidos pela Contratante.

6.10.2. O contrato indicará o serviço, a quantidade e a localidade onde será prestado o serviço.

6.10.3. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana, conforme estipulado no requisito de manutenção.

6.10.4. A execução do serviço deve ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

6.10.5. A CONTRATADA deverá fornecer número telefônico e e-mail para contato e registro de ocorrências sobre o acompanhamento do serviço contratado.

6.10.6. A Contratante será a responsável pela verificação da aderência aos padrões de qualidade exigidos dos produtos entregues.

6.11. Requisitos de Segurança da Informação e Privacidade

6.11.1. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

6.11.1.1. Respeitar a adequação à legislação vigente, tais como a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014).

6.11.1.2. A solução contratada deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.

6.11.1.3. A Contratada deverá manter a integridade da rede de dados e das informações da MB durante a prestação dos serviços.

6.11.1.4. A Contratada deverá respeitar a Política de Segurança da Informação e Comunicações da MB, bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato.

6.11.1.5. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do objeto, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo CONTRATANTE a tais documentos.

6.12. Observância às Vedações da IN SGD/ME nº 94/2022

6.12.1. A área técnica declara ter analisado as disposições constantes nos arts. 3º, 4º e 5º da Instrução Normativa SGD/ME nº 94/2022, não tendo identificado vedação aplicável que impeça a presente contratação.

6.12.2. A presente contratação refere-se à renovação de licenças, subscrições, suporte técnico e garantia de soluções de segurança cibernética já implantadas na infraestrutura da RECIM, destinando-se à manutenção da continuidade operacional, atualização tecnológica e preservação da segurança da informação institucional.

6.12.3. As referências às soluções, equipamentos e ecossistemas atualmente empregados decorrem de requisitos de compatibilidade técnica, preservação dos investimentos realizados, continuidade operacional, integração com o ambiente existente, manutenção das políticas de segurança implementadas e mitigação de riscos operacionais e cibernéticos, não configurando direcionamento indevido ou restrição injustificada à competitividade.

6.12.4. A área técnica declara, ainda, não ter identificado, até a presente etapa da instrução processual, norma específica adicional do Órgão Central do SISP aplicável ao objeto, além das disposições gerais previstas na IN SGD/ME nº 94/2022 e demais normativos aplicáveis às contratações de soluções de TIC.

6.13. Requisitos complementares da contratação

6.13.1. Padrões mínimos de qualidade e desempenho

As licenças, subscrições, atualizações, suporte técnico e garantia deverão atender integralmente às especificações técnicas previstas no Termo de Referência, assegurando compatibilidade com as soluções IPS Trellix NS9500 e Firewall Cisco Firepower 2140 atualmente implantadas na RECIM, sem necessidade de aquisição adicional de hardware, alteração de topologia ou reconfiguração estrutural das políticas de segurança já estabelecidas.

6.13.2. A solução deverá preservar, no mínimo, a capacidade de atualização de assinaturas, correções de segurança, suporte técnico, garantia/RMA quando aplicável, geração de logs, registro de eventos, monitoramento, auditoria e manutenção da capacidade de inspeção, prevenção e bloqueio de ameaças cibernéticas.

6.13.3. Utilização do Catálogo Eletrônico de Padronização

Foi avaliada a possibilidade de utilização do Catálogo Eletrônico de Padronização de Compras, Serviços e Obras do Governo Federal. Considerando que o objeto consiste na renovação de licenças, subscrições, atualização, suporte e garantia de soluções específicas de segurança de borda já implantadas na RECIM, não foi identificado item padronizado que substitua integralmente a especificação necessária sem risco à compatibilidade técnica, continuidade operacional, suporte e preservação dos investimentos já realizados. A consulta deverá ser registrada nos autos pela área competente.

6.13.4. Atendimento ao princípio da padronização

A contratação atende ao princípio da padronização, previsto no art. 40, inciso V, alínea "a", da Lei nº 14.133/2021, pois mantém a compatibilidade com o parque tecnológico existente, evita substituição prematura de ativos em operação, preserva políticas de segurança já configuradas, aproveita a capacitação técnica da equipe, reduz riscos de indisponibilidade e assegura continuidade da proteção cibernética da RECIM.

6.13.5. Critérios e práticas de sustentabilidade

Considerando que o objeto consiste predominantemente em renovação de licenças, subscrições, atualizações de segurança, suporte técnico e garantia de soluções já implantadas, não há aquisição principal de novos equipamentos, razão pela qual os impactos ambientais diretos são reduzidos. Quando houver substituição de componentes, módulos, acessórios ou equipamentos em razão de garantia, suporte ou RMA, a contratada deverá observar, no que couber, a destinação ambientalmente adequada de resíduos eletroeletrônicos, a redução de embalagens, a reutilização ou reciclagem de materiais e as normas ambientais aplicáveis.

6.13.6. Amostra ou prova de conceito

Não será exigida amostra ou prova de conceito, considerando que se trata de renovação de licenças, subscrições, suporte e garantia de soluções já implantadas e em uso pela Administração. A conformidade será verificada por meio da análise da proposta, catálogos técnicos, declaração do fabricante, comprovação de licenciamento, documentação de elegibilidade para suporte ou documento equivalente, o que se mostra suficiente e menos oneroso ao certame.

6.13.7. Subcontratação

Não será admitida a subcontratação do objeto, pois a contratação envolve fornecimento, renovação e ativação de licenças/subscrições, suporte técnico e garantia vinculados à cadeia de responsabilidade da contratada, do fabricante ou de rede autorizada. A vedação busca preservar a rastreabilidade do licenciamento, a autenticidade das chaves ou autorizações de uso, a integridade do suporte, a segurança da informação e a responsabilidade técnica perante a Administração.

6.13.8. Natureza acessória da contratação

A contratação possui natureza instrumental, acessória e complementar às atividades institucionais da Marinha do Brasil, pois visa manter operacionais as soluções de segurança cibernética que protegem a infraestrutura de TIC da RECIM. O objeto não implica delegação de atividade estratégica, decisória, típica de Estado ou própria da área de competência institucional, restringindo-se ao suporte tecnológico necessário à continuidade e à segurança dos serviços de TIC.

6.14. Justificativa para não adoção do Sistema de Registro de Preços

A presente contratação não será processada pelo Sistema de Registro de Preços, tendo em vista que a demanda da Administração é certa, previamente delimitada e integralmente conhecida.

6.14.1. O objeto refere-se à renovação de licenças, subscrições, suporte técnico e garantia de soluções de segurança cibernética específicas já implantadas na infraestrutura da RECIM, possuindo quantitativos definidos e necessidade imediata de contratação, não havendo imprevisibilidade de consumo que justifique a adoção do Sistema de Registro de Preços.

6.14.2. Ademais, a contratação visa assegurar a continuidade operacional e a manutenção da capacidade de proteção da infraestrutura de TIC institucional, sendo mais adequada a contratação por pregão eletrônico tradicional, com fornecimento integral das licenças e serviços necessários ao atendimento da demanda identificada no planejamento da contratação.

6.14.3. Registra-se, ainda, que a adoção do Sistema de Registro de Preços não apresentaria ganhos de economicidade ou eficiência administrativa no caso concreto, considerando a natureza específica, delimitada e certa da demanda, que não se destina ao atendimento de necessidades futuras, incertas ou de múltiplos órgãos.

6.15. Condições de pagamento

As condições de pagamento foram definidas em observância às práticas correntes do mercado para contratação de licenças, subscrições, suporte técnico, atualização e garantia de soluções de segurança cibernética, considerando a natureza do objeto, a forma usual de fornecimento por ativação ou disponibilização eletrônica e a necessidade de preservar a atratividade do certame, a competitividade, a isonomia e a seleção da proposta mais vantajosa para a Administração.

6.15.1. O pagamento será realizado conforme previsto no Termo de Referência, após a assinatura do contrato ou instrumento equivalente, apresentação da Nota Fiscal/Fatura pela contratada e regular ateste pela fiscalização competente, observadas as condições de recebimento provisório e definitivo.

7. Estimativa da demanda - quantidade de bens e serviços

A Marinha do Brasil conta com uma infraestrutura de TI que visa atender cerca de 60.000 (sessenta mil) usuários civis e militares, além de 57 (cinquenta e sete) firewalls e 7 (sete) equipamentos de Intrusion Prevention System (IPS) distribuídos por toda a RECIM.

Por se tratar de uma instituição estabelecida em todo o território nacional bem como, em escritórios internacionais, além de postos de observação remotos, navios e base de pesquisa no continente Antártico, e que também lida com projetos altamente sigilosos que afetam a segurança nacional, o trato com a segurança da informação requer uma solução de IPS, mas além disso, requer uma solução que permita a continuidade dos serviços sem mudanças abruptas e/ou que possam gerar gargalos de conhecimento, uma vez que esta instituição já adota solução Trellix Network Security Platform ao longo de mais de 10 anos e a solução de firewall da Cisco a mais de 20 anos, em toda a sua infraestrutura de TI.

A Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), na qualidade de Diretoria Especializada, responsável pelas atividades relativas à Segurança da Informação e Comunicações da MB, necessita manter atualizados os equipamentos IPS e firewall, atualmente instalados e em uso.

A manutenção das licenças dos dois equipamentos que fazem parte da solução de segurança de borda da RECIM visa manter a implementação de uma primeira e segunda camada de infraestrutura de Segurança, possibilitando o controle, monitoração, identificação e prevenção de padrões de comportamento e tentativas de intrusões aos serviços disponibilizados na Internet, como premissa básica para que se estabeleça um perímetro seguro e elementar aos nossos sistemas de missão crítica.

A ausência da solução de firewall e IPS atualizado reduziria a capacidade de proteção cibernética da rede, da MB, reduzindo sua capacidade de cumprir com suas obrigações constitucionais, tais como a salvaguarda da vida humana do mar e a prestação de serviço à população. Desta forma, é primordial a renovação das licenças de serviço de suporte/atualização e gerência dos sensores.

A demanda da Administração consiste em manter as licenças de serviço de atualização/suporte e garantia de troca de equipamento ou de componentes, considerando-se as quantidades necessárias para apenas dois equipamentos que compõem a segurança da borda de acesso à RECIM, que poderão parar de receber *patches* de atualizações e, por conseguinte, o suporte do fabricante. Atualmente, tornou-se de suma importância manter os equipamentos de segurança cibernética atualizados, a fim de mitigar possíveis ações de cibercriminosos. Além disso, a partir de 2020 ocorreu um investimento de R\$ 2.429.000,00 e de R\$ 5.465.563,00 na troca de todos os equipamentos/licenças IPS e firewall, respectivamente, pois os aparelhos em produção encontravam-se com end of life anunciado.

Desta forma, é de suma importância renovar as licenças em uso na MB dos equipamentos: IPS modelo 9500 e do firepower 2140 instalados na borda da RECIM.

O uso da solução IPS possibilita à MB a manutenção da visualização global dos níveis de segurança em que se encontra a RECIM e possibilita a tomada de ações imediatas para adequá-la a níveis de segurança aceitáveis.

A ausência da solução IPS e firepower atualizada reduziria a capacidade de proteção cibernética da rede, da MB, reduzindo e impactando o cumprimento de suas obrigações constitucionais, tais como a salvaguarda da vida humana no mar e a prestação de serviço à população. Desta forma, é primordial a renovação das licenças de serviço de suporte/garantia e atualização.

Neste contexto, o presente Estudo Técnico Preliminar aponta a necessidade de implementar uma solução de segurança de acordo com as necessidades de negócio e tecnológicas apontadas nos itens 4 e 5 deste estudo. Para isso, faz-se necessária a contratação dos seguintes itens:

Item	DESCRIÇÃO	QUANTIDADE
1	Subscrição de licenças de autorização de uso/atualização/suporte e garantia de troca de equipamento ou de componentes do mesmo em produção.	8

A quantidade apresentada, na tabela anterior, para o item 1, corresponde a 8 licenças, levando em consideração a demanda atual de manter os appliances cobertos com atualização/suporte e garantia de troca do equipamento de IPS e firewall em produção na Rede de Comunicações Integrada da Marinha (RECIM).

Sendo assim, a demanda se divide da seguinte forma:

- 3 (três) unidades de subscrição de licenças de autorização para direito de uso e atualização do software, utilizadas no equipamentos IPS NS-9500 e firepower 2140;
- 3 (três) unidades de licenças para suporte e direito de autorização e substituição dos appliances modelo IPS-NS 9500 e firepower 2140; e
- 2 (duas) unidades de licenças para suporte e direito de autorização de substituição dos módulos GBIC para o appliance modelo IPS-NS 9500.

Parcelamento

A contratação será realizada com parcelamento parcial do objeto, considerando a existência de soluções tecnologicamente distintas no ambiente de segurança de borda da Rede de Comunicações Integrada da Marinha (RECIM), especialmente entre os ecossistemas Firewall Cisco Firepower e IPS Trellix NS9500.

O parcelamento foi adotado de forma a ampliar a competitividade e permitir a disputa individualizada entre soluções independentes, observando-se o disposto no art. 47 da Lei nº 14.133/2021 e no art. 12, §3º, da IN SGD/ME nº 94/2022.

Entretanto, os itens vinculados à solução IPS Trellix NS9500 não comportam fracionamento adicional entre si, tendo em vista a elevada interdependência técnica existente entre licenças, módulos, suporte, garantia e funcionalidades associadas ao equipamento atualmente em produção na RECIM.

A segregação desses componentes poderia gerar incompatibilidades de cobertura, dificuldades de acionamento de garantia e suporte, fragmentação de responsabilidades, riscos de descontinuidade operacional e falhas na atualização coordenada das assinaturas e funcionalidades de segurança da solução IPS.

Além disso, a solução atualmente implantada possui políticas, integrações e configurações já consolidadas no ambiente institucional, sendo necessária a preservação da compatibilidade técnica e operacional do ecossistema existente, sem alteração de topologia, arquitetura ou funcionalidades implementadas.

Dessa forma, adotou-se o parcelamento apenas entre soluções tecnologicamente independentes, mantendo-se agrupados os itens diretamente relacionados ao ecossistema IPS Trellix NS9500, por constituírem conjunto técnico integrado e indissociável para fins de funcionamento, suporte e continuidade da proteção cibernética da RECIM.

8. Levantamento de mercado

8.1. Manifestação sobre a Vantajosidade da Aquisição frente à Locação

Em estrita observância ao art. 44 da Lei nº 14.133/2021, esta área técnica certifica expressamente que a aquisição dos bens descritos neste estudo demonstra-se a opção mais vantajosa para a Administração Pública em detrimento de alternativas como a locação de bens. A justificativa pauta-se nos seguintes fatores:

- I - Natureza do objeto: a contratação pretendida refere-se à renovação de licenças/subscrições e serviços agregados de suporte, atualização e garantia, indispensáveis à continuidade operacional dos equipamentos Firewall Cisco FPR2140 e IPS Trellix NS9500. Assim, não há bem a ser

locado para atendimento da demanda, mas sim a necessidade de manter ativos os direitos de uso, atualização, suporte técnico e garantia vinculados às soluções já pertencentes ou em uso pela Administração;

II - Inaplicabilidade da locação: a locação de novos equipamentos não se mostra adequada pois implicaria substituição ou sobreposição de solução tecnológica já implantada, com necessidade de migração, homologação, reconfiguração de políticas de segurança, adaptação operacional e eventual capacitação técnica adicional, além de risco de descontinuidade dos serviços de proteção cibernética durante a transição;

III - Aspecto econômico e preservação dos investimentos: a renovação das licenças, subscrições, suporte técnico, atualização e garantia preserva os investimentos realizados pela Administração, evita substituição prematura de ativos em operação, mantém a compatibilidade com o ambiente tecnológico existente e reduz custos indiretos associados à implantação de nova solução; e

IV - Continuidade operacional: a manutenção das licenças e coberturas atualmente necessárias assegura a continuidade das atualizações de segurança, do suporte técnico, da garantia e da capacidade de inspeção, prevenção e bloqueio de ameaças cibernéticas, reduzindo riscos de indisponibilidade da solução de segurança de borda da RECIIM.

Dessa forma, conclui-se que, diante da natureza do objeto, a renovação das licenças, subscrições, suporte técnico, atualização e garantia das soluções atualmente implantadas apresenta-se como alternativa técnica e economicamente mais adequada ao atendimento da necessidade pública, não sendo aplicável a locação de bens ou equipamentos para o caso concreto.

9. Levantamento de soluções

9.1. Solução 1: Renovação das licenças dos equipamentos IPS e firewall da solução de segurança do fabricante Trellix e Cisco, respectivamente.

A MB adota solução do IPS do fabricante Trellix (antiga McAfee) há mais de 10 anos, e atualmente, possui distribuídos, em todo território nacional, equipamentos de hardware (sensores) componentes do sistema de segurança de rede “Trellix Network Security Platform – Intrusion Prevention System (IPS)”, os quais, proveem fator adicional e imprescindível de proteção às redes de dados desta Força, atuando contra ações maliciosas como: a propagação de atividades relacionadas a malware (arquivos maliciosos, vírus, etc), negação de serviço (interrupção da comunicação, na rede de dados, por quantidade desmensurada de requisições anômalas, por vezes provenientes de origens múltiplas na internet - DDoS), ataques diversos a sistemas digitais, ameaças sofisticadas etc.

Os firewalls de categoria Next-Generation firewall (NGFW) correspondem a uma plataforma de rede integrada, baseada em inspeção profunda (deep packet inspection), provendo múltiplos mecanismos de proteção em um único equipamento, Inspeção em nível de aplicação e usuários, Inspeção de SSL/SSH, VPN, Filtro de Websites e Gerenciamento de banda (QoS).

Um NGFW oferece controle granular de aplicativos, e também fornece segurança contra as ameaças representadas por ataques de malware sofisticados e evasivos. Ele oferece gerenciamento abrangente e unificado de políticas de funções de firewall, controle de aplicativos, prevenção de ameaças e proteção avançada contra malware da rede ao terminal. Além de prover a centralização das inspeções e correlação de logs ainda entrega performance para redes de grande porte. O NGFW permite: instalação in-line sem perda de performance; capacidades de firewall de primeira geração (Ex. NAT, Stateful Inspection Protocol, VPN, etc.); visibilidade de aplicativos de forma granular e descriptografia SSL para permitir a identificação de aplicações criptografadas indesejadas.

A solução NGFW Cisco conta com o appliance Firepower Threat Defense (FTD), que possui diversas séries de modelos. Cada série visa atender uma certa demanda de volume de tráfego esperado, no caso deste estudo seria para atender a demanda do appliance firepower 2140.

O atual sistema de proteção cibernética da MB, possui características desejadas e requisitos de segurança adequados e necessários à continuidade das atividades da MB, dentre os quais:

- inspeção de tráfego WEB criptografado SSL, visando identificar ameaças que se utilizem deste artifício para evasão das rotinas de inspeção e de reconhecimento de atividades maliciosas;
- proteção contra ataques de Negação de Serviço (DoS – Deny of Service e DDoS – Distributed Denial of Service); e
- recursos de análise e de prevenção integrada de ameaças.

Adicionalmente, a referida solução atende aos requisitos desejados de performance e de gerenciamento, como:

- escalabilidade de desempenho em cenários que exigem redimensionamento para atendimento de demanda em redes de alta capacidade;
- throughput mínimo de 9 Gbps;
- alta disponibilidade; e
- gerenciamento centralizado.

A implantação da atual solução IPS e firewall, na MB, incluiu as fases de: homologação da solução; testes de funcionamento em rede; adaptações (customizações) para atendimento das especificidades de sigilo da MB; implantação de sensores em Organizações Militares diversas em todo o território nacional e treinamento/capacitação de pessoal.

Os altos investimentos financeiros nos equipamentos e em capacitação de pessoal, outrora realizados em prol das atividades de defesa cibernética, permitiram que a MB, hoje, mantenha a segurança de suas redes de dados e dê continuidade às atividades e projetos de interesse da Força, possibilitando a implantação e a alteração de políticas de segurança, em sua rede de dados, com menor tempo e maior acurácia. O aperfeiçoamento técnico alcançado é fruto de persistência e constante dedicação, visto que, a introdução de uma nova tecnologia requer, conforme representação da curva de aprendizagem, maior tempo despendido para seu domínio.

Faz-se necessário considerar que, para o referido cenário, a MB precisa renovar 5 (cinco) itens, totalizando 8 (oito) unidades/licenças de atualização, suporte e garantia das soluções Trellix e Cisco, preservando assim o investimento iniciado em 2020 com a troca dos equipamentos e a capacitação da equipe.

Essa alternativa tem como objetivo manter a arquitetura do Sistema IPS e firewall atualmente em produção na MB.

9.2. Solução 2A: Adoção da plataforma de segurança de rede e de prevenção à intrusão Trend Micro TippingPoint IPS.

A família TippingPoint Threat Protection System, composta por soluções e softwares de Prevenção de Intrusões (IPS) empresariais da Trend Micro, é amplamente reconhecida e bem conceituada no mercado, integrando um portfólio de soluções de empresas líderes em Tecnologia da Informação (TI) e cibersegurança.

O Trend Micro TippingPoint IPS oferece funcionalidades como detecção, proteção e mitigação de ameaças em tempo real, além da capacidade de eliminar pontos cegos de SSL por meio da inspeção de tráfego criptografado, sem comprometer o desempenho da rede. Esses e outros recursos também já estão presentes nos sistemas IPS atualmente utilizados pela Marinha do Brasil.

9.3. Solução 2B: Firewall UTM

O conceito de Firewall UTM (Unified Threat Management) surgiu em resposta à evolução do mercado de segurança da informação e às crescentes demandas por proteção mais abrangente. À medida que novas ameaças e vulnerabilidades eram identificadas, os firewalls passaram a incorporar recursos e funcionalidades adicionais, ampliando sua capacidade de defesa.

Por causa disso, um UTM pode ser facilmente identificado como um ativo de software e hardware – ou uma combinação entre os dois – que centraliza em uma única plataforma, várias características, tais como:

- Solução Firewall;
- Filtragem Stateful;
- VPN;
- Proxy Web;
- Antivírus;
- IDS/IPS;
- Balanceamento de carga;
- Relatórios e logs; e
- Inspeção profunda de pacote (DPI).

Como limitação ao Firewall UTM, podemos destacar problemas associados a performance, uma vez que todas as funções de segurança estão centralizadas em um único produto. O problema geralmente acontece em ambientes corporativos com alto volume de pacotes e hardwares insuficientes. Dessa forma, existem prejuízos no processamento das regras de segurança aplicadas no ambiente.

Referência: <https://ostec.blog/seguranca-perimetro/firewall-utm-ngfw-diferenca/>

9.4. Solução 3: Aquisição hardware para hospedar software livre do IPS e firewall NGFW

Para esta solução a MB, adotaria a seguinte estratégia: passaria a utilizar software livre para monitorar e detectar a presença de atividades intrusivas. Todavia, esta abordagem demandaria a aquisição de vários servidores e da instalação de software gratuito (como o open-source Snort) em substituição aos appliances IPS e firewall adquiridos a partir de 2020.

Neste contexto, o uso de software livre exigiria foco não só na ferramenta, mas também no ambiente em que ela funciona. Cabe acrescentar que soluções em software livre não proveem interfaces adequadas para garantir a facilidade de uso e orquestração. Ademais, ao se adotar tal solução, existe também a necessidade de gerência de recursos do próprio sistema operacional que a hospeda, como logs, configuração de arquivos e envio de logs para base centralizada. Embora não haja custo na aquisição do software em si, há

um significativo custo operacional indireto com o acréscimo de trabalho de configuração e manutenção, além do custo de aquisição do hardware e treinamento necessários.

Além disso, soluções IPS e firewall NGFW de uso gratuito não garantem que as mais recentes atualizações (quando não adicionadas ou vinculadas a um serviço pago) estarão disponíveis ao público em geral com brevidade e acurácia. No caso do Snort, um dos mais conhecidos softwares gratuitos do ramo, hoje adquirido pela gigante empresa Cisco, sua adoção em ambientes críticos e heterogêneos e que demandem alta disponibilidade, requeiram redes de alta velocidade, resiliência, hardware dedicado etc, pode configurar-se como inviável e ineficiente, frente às soluções proprietárias e suas funcionalidades como integração, gerência centralizada, inspeção de tráfego criptografado SSL, analisadores de malwares, tolerância a falhas e outras.

A adoção da solução Snort, por tratar-se de software instalado em um servidor, por vezes virtualizado, e cujo tráfego de dados é realizado, obrigatoriamente “em linha”, pode ocasionar, eventualmente, a interrupção de toda a rede da MB em caso de falhas (elétrica, de software/hardware etc), visto que, funcionalidades que permitam a continuação do tráfego de dados, como “fail open”, para redes /ativos não afetados não estarão disponíveis. Para tratar este risco, é necessária uma estratégia de continuidade do serviço do tipo tolerância a falhas (failover), na qual exista redundância automática entre os equipamentos da solução.

É importante mencionar que as soluções baseadas em software livre não são suficientes para atender a necessidade de prevenção e proteção das redes envolvidas com perfil de eficiência e proatividade requeridos pela MB. Haveria pois a necessidade de maior atuação de equipes de profissionais de rede para a devida inspeção, bloqueio, contorno de problemas etc.

Do ponto de vista da segurança da rede corporativa da MB, para que o uso de soluções livres seja viável, é necessário não só aumento de capacidade de processamento, mas também o aumento e a capacitação do corpo técnico da área de tecnologia da informação do Centro de Tecnologia da Informação da Marinha (CTIM). A especialização nestas tecnologias é mais complexa, difícil de conseguir e requer tempo para o aprendizado, amadurecimento e domínio. Esse cenário, aliado ao fato de não termos suporte terceirizado para lidar com essas novas soluções, ressalvada a hipótese de mera operacionalização, tornando a alternativa em tela vulnerável à falhas e ao não atendimento dos objetivos.

10. Análise comparativa de soluções

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

arquivísticos)	Solução 3			X
A solução possui poder de inspeção de tráfego capaz de suporta grande volume?	Solução 1	X		
	Solução 2A	X		
	Solução 2B	X		
	Solução 3		X	
A solução manterá o parque tecnológico referente aos IPS distribuídos, atualmente, na MB, em plena operação, com as devidas atualizações de segurança e suporte remoto?	Solução 1	X		
	Solução 2A		X	
	Solução 2B			X
	Solução 3		X	
A solução manterá o parque tecnológico referente aos firewall distribuídos, atualmente, na MB, em plena operação, com as devidas atualizações de segurança e suporte remoto?	Solução 1	X		
	Solução 2A			X
	Solução 2B		X	
	Solução 3		X	

11. Registro de soluções consideradas inviáveis

Solução 2A: Adoção da plataforma de segurança de rede e de prevenção à intrusão Trend Micro TippingPoint IPS.

A adoção da referida solução implicaria, necessariamente, na aquisição de novos equipamentos compatíveis com o ecossistema Trend Micro TippingPoint, bem como na adesão ao seu sistema de gerenciamento e na obtenção de todas as licenças adicionais requeridas. Tal decisão desconsideraria os investimentos já realizados pela Marinha do Brasil na plataforma Trellix, incluindo capacitação de pessoal e infraestrutura atualmente em uso, gerando elevado impacto gerencial, financeiro e de segurança sobre o patrimônio digital da MB, além do tempo necessário para implementação, adaptação e treinamento da equipe.

Solução 2B: Firewall UTM

Este tipo de firewall deve ser composto com uma solução de Ameaça Persistente Avançada, o que implica na necessidade de, pelo menos, dois diferentes fabricantes. A existência de equipamentos de diferentes fabricantes acarreta em incremento nos custos operacionais e de treinamentos, além de inviabilizar o gerenciamento integrado, já que os softwares de gerência não são criados com este intuito, o que nos conduz a algumas limitações quando analisada a solução composta por múltiplos fabricantes.

Além disso, para grandes empresas e instituições, um dispositivo UTM pode apresentar problemas de performance, uma vez que os recursos do hardware são compartilhados entre vários serviços.

Solução 3: Aquisição de hardware para hospedar software livre do IPS e firewall NGFW

Pelo exposto, na apresentação da solução 3, esta também não atende. Pelo fato de ter uma abordagem com uso exclusivo de software livre não só implicaria em custos de aquisição de hardware, como adicionaria risco inaceitável de indisponibilidade, além de aumentar o custo operacional, com o qual esta instituição não poderia arcar, dado seu quadro restrito de militares alocado para atendimento de a toda a MB. Destaque-se, ainda, que as soluções livres existentes não são capazes de atender a todos os requisitos de segurança requeridos pelas melhores práticas de segurança da informação sob o ambiente da MB.

Entende-se, portanto, que o uso de software livre só seria possível, no máximo, como item complementar à gestão da segurança da informação, e não como sua principal fonte de gerência.

12. Análise comparativa de custos (TCO)

Durante este estudo, verificou-se a intenção de adquirir a solução 1 por um período de 3 (três) anos, devido aos descontos progressivos aplicados. Porém, devido ao cenário econômico desfavorável, previsto para 2026, e além de tratar-se de uma solução imprescindível em qualquer Órgão Público, a MB somente poderá adquirir o objeto, por 12 (doze) meses, com pagamento único, pois o fabricante, em relação à licença, somente trabalha desta forma.

Para a definição do preço estimado do objeto deste ETP, foram seguidos os procedimentos administrativos estabelecidos pela Instrução Normativa SEGES/ME nº 65/2021, que trata da pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional, além dos dispositivos relevantes da mesma Instrução Normativa.

Dessa forma, a equipe técnica deste ETP realizou uma pesquisa de preços conforme estabelecido na Instrução Normativa nº 73, de 5 de agosto de 2020, que regula o procedimento administrativo para a pesquisa de preços na aquisição de bens e contratação de serviços no âmbito da administração pública federal direta, autárquica e fundacional, apenas da solução 1, porque foi considerada viável, por ser a única que atende a todas as necessidades de negócio e tecnológicas, conforme demonstrado na tabela do item 9 deste documento.

Em relação, aos itens 1, 2 e 3 as consultas relacionadas foram realizadas nos sites governamentais <https://www.gov.br/compras/pt-br/aceso-a-informacao/consulta-detalhada> e <https://pncp.gov.br/app/editais?pagina=1> no dia 01/04/2026 às 10hrs, utilizando como termo de pesquisa "MFE Net Sec IPS-NS9500 e MFE NS9500", no período de 01/04/2025 a 01/04/2026, conforme consta no anexo I do ETP. Como se trata de um produto com grande especificidade funcional, há pouca variação nos termos de busca, e o resultado foi que não houve nenhuma licitação.

Apesar da ampliação do período de pesquisa para sem período de publicação, conforme consta no anexo I do ETP, como mostrado abaixo na Tabela 1, indicou a ocorrência de um pregão desta Diretoria, ocorrido em 2020.

Tabela 1

TABELA RESUMO						
ID	CONTRATAÇÕES SIMILARES ENCONTRADAS	ITENS	DESCRIÇÃO	QUANTIDADE	CUSTO UNITÁRIO	VALOR TOTAL PREGÃO
1	PE Nº 07/2020 DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA DA INFORMAÇÃO DA MARINHA (UASG: 749000) Processo Administrativo: 63394.000727/2020-82 ANO/MÊS DA LICITAÇÃO: AGO2020	1	MFE Net Sec IPS- NS9500 Appl 1Yr ARMA	1	R\$ 135.150,00	R\$ 135.150,00
		2	MFE NS9500 (10Gbps) Perp Lic	1	R\$ 498.000,00	R\$ 498.000,00
		3	MFE NS9500 (10Gbps) 1Yr BZ	1	R\$ 298.400,00	R\$ 298.400,00

As consultas relacionadas aos itens 4 e 5 foram realizadas no site governamental <https://www.gov.br/compras/pt-br/aceso-a-informacao/consulta-detalhada> e <https://pncp.gov.br/app/editais?pagina=1> no dia 01/04/2026 às 10hrs, utilizando como termo de pesquisa "Licença Cisco Firepower 2140", no período de 01/04/2025 a 01/04/2026, conforme consta no anexo I do ETP, e uma pesquisa sem período de publicação, anexo I. No primeiro resultado da pesquisa não apareceu nada, já na segunda pesquisa obtivemos o resultado da Tabela 2 abaixo. Como se trata de produto com grande especificidade funcional, há pouca variação dos termos para buscas.

Tabela 2

TABELA RESUMO						
ID	CONTRATAÇÕES SIMILARES ENCONTRADAS	ITENS	DESCRIÇÃO	QUANTIDADES	CUSTO UNITÁRIO	VALOR TOTAL PREGÃO
1	PE Nº 33/2023 CENTRO LOGÍSTICO DO MATERIAL DA MARINHA (UASG: 740014) Processo Administrativo: 63394.000608/2023-72 ANO/MÊS DA LICITAÇÃO: OUT2023	1	Licença Cisco FPR2140 Threat Defense Threat, Malware and URL 3Yr	2UN	R\$ 340.000,00	R\$ 680.000,00

Devido os valores encontrados nas licitações supracitadas na Tabela 1 ter acontecido a mais de 5 anos e da Tabela 2 a mais de 2 anos atrás, e a variação cambial durante estes anos ter variado muito, necessitou não considerar os parâmetros do artigo 5º, incisos I e II da IN Seges/ME nº 65/2021 como prioridade.

Desta forma, a fim de evitar distorções nos valores estimados máximo deste processo e a licitação não ser deserta, pois trata-se de soluções essenciais para os equipamentos de segurança cibernética instalados na borda da RECIM em plena condições operacionais, fez-se necessário complementar essa pesquisa de preços com consultas diretas aos fornecedores.

Dessa forma, foram solicitadas cotações por e-mail às empresas parceiras dos fabricantes Trellix e Cisco, sendo: 4 (quatro) consultas para os itens 1, 2 e 3 da solução Trellix; e 5 (cinco) consultas para os itens 4 e 5 da solução Cisco, conforme Anexo II do ETP. Em relação às consultas encaminhadas, registrou-se que, para a solução Trellix, a empresa Xsite não respondeu e a AboutNet declinou da apresentação de proposta; e, para a solução Cisco, a empresa Toptech não respondeu.

Na solicitação de orçamento, com a finalidade de verificar a vantajosidade econômica da contratação em maior período de vigência com pagamento único, foram solicitadas propostas para 12, 24 e 36 meses. Após o recebimento das propostas, foi elaborado o mapa comparativo de preços com base nos orçamentos apresentados pelas empresas Netsafe Corp, Future, NTT, Scansource, GLOBALSEC e World Partners, constante do Anexo IV do ETP.

Embora se verifique que a contratação por 36 meses apresente maior vantajosidade econômica e administrativa, há previsão de disponibilidade orçamentária apenas para a contratação de 12 meses, no exercício de 2026.

Devido ao mercado se restringir apenas aos parceiros do fabricante Trellix e Cisco, a equipe avaliou no mapa comparativo, que é mais vantajoso utilizar o menor valor para compor o valor máximo unitário, uma vez que as empresas parceiras na qual enviaram as propostas com menores valores são consolidadas no mercado, ou seja, existe a possibilidade de baixar os valores durante o pregão e outras empresas que não receberam o e-mail de solicitação de orçamento no momento do pregão participarem do mesmo.

Acrescenta-se, por fim, que integra a instrução do processo o Documento de Formalização da Pesquisa de Preços, constante do Anexo V do ETP.

12.1. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Conforme demonstrado no presente estudo, apenas a solução 1 foi classificada como viável. Dessa forma, a tabela abaixo apresenta o TCO dessa solução, com base nos valores da coluna “Total” apresentados no Mapa Comparativo, anexo IV do ETP, na qual foi montada com os valores informados nos orçamentos recebidos, constante anexo III do ETP.

Descrição da solução	Estimativa de TCO ao longo dos anos				TOTAL R\$
	Ano 1	Ano 2	Ano 3	Ano 4	
	(Licenças)	+ ICTI (3,12%)	+ ICTI (3,12%)	+ ICTI (3,12%)	
	R\$	R\$	R\$	R\$	
SOLUÇÃO 1	770.171,08	794.200,41	818.979,47	844.531,63	3.227.882,59

Índice de Custo da Tecnologia da Informação (ICTI): o percentual de 3,12% corresponde ao acumulado dos últimos 12 meses disponíveis (fevereiro de 2025 a fevereiro de 2026), considerando a indisponibilidade do dado referente a março de 2026.

13. Descrição da solução de TIC a ser contratada

13.1. Conforme demonstrado no presente estudo, apenas a solução 1 é encaminhada como solução viável.

13.2. Visando a preservação do investimento iniciado em 2020 com equipamentos dos IPS e firewall, suas licenças e treinamento, a solução 1 seria a alinhada com o Requisito de Negócio nº 1, sendo necessário manter o parque tecnológico referente à solução *Trellix Network Security Platform – Intrusion Prevention System (IPS)* e da solução Cisco, na Marinha do Brasil (MB), em plena operação, com as devidas atualizações de segurança e suporte remoto e esta solução também segue a linha de investimentos realizada até hoje com os demais equipamentos de rede que a MB já possui.

13.3. A solução prevê a aquisição de:

13.3.1. 3 (três) unidades de subscrição de licenças de autorização para direito de uso e atualização do software, utilizadas nos equipamentos IPS NS-9500 e Firepower 2140;

13.3.2. 3 (três) unidades de licenças para suporte e direito de autorização e substituição dos appliances modelo IPS-NS 9500 e firepower 2140; e

13.3.3. 2 (duas) unidades de licenças para suporte e direito de autorização de substituição dos módulos GBIC para o appliance modelo IPS-NS 9500.

13.4 Assim, a solução de TIC a ser contratada é composta por 5 (cinco) itens, totalizando 8 (oito) unidades/licenças, voltados à atualização, suporte e garantia das soluções IPS Trellix NS9500 e Firewall Cisco Firepower 2140 em produção na RECIM.

14. Estimativa de custo total da contratação

Valor (R\$): 770.171,08

De acordo com apresentado anteriormente, através das estimativas de custos de menor valor de cada item entre as propostas apresentadas pelas empresas, o custo para contratação (manutenção das licenças de uso, atualização, suporte e garantia de troca de alguns dos equipamentos em uso na MB) é de R\$ 770.171,08 (setecentos e setenta mil cento e setenta e um reais e oito centavos).

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO R\$	VALOR DE TOTAL R\$
1	MFE Net Sec IPS-NS9500 Appl ARMA	27740	UN	1	60.000,00	60.000,00
2	NS 4port FO Mod 10-1GigE 850nm 50um RMA	27740	UN	2	10.000,00	20.000,00
3	MFE NS9500 (10Gbps)	27502	UN	1	130.000,00	130.000,00
4	Cisco FPR2140 Threat Defense Threat, Malware and URL	27502	UN	2	192.327,55	384.655,10
5	Cisco Firepower 2140 SOLN SUPP 8X5XNBD (Suporte e Garantia)	27740	UN	2	87.757,99	175.515,98
TOTAL GERAL						770.171,08

15. Justificativa técnica da escolha da solução

15.1. Como demonstrado ao longo deste estudo, atualmente a MB conta com uma solução de IPS baseada totalmente na plataforma do fabricante Trellix e uma solução de firewall do fabricante Cisco, ambas usadas na MB, há mais de 10 anos, além de ter equipe que possui conhecimento técnico nas ferramentas de IPS e firewall destes fabricantes supracitados. A opção por estas soluções permitirá que esta instituição mantenha o sensor principal de IPS e o *appliance* do Firewall atualizado, com suporte e garantia de troca, tanto quanto manter elevado o nível de controle e detecção de ameaças que aumentam cada vez mais nas camadas mais altas dos pacotes trafegados.

15.2. Como verificado, tratam-se de soluções de TI essenciais para assegurar a proteção da RECIM, garantindo desempenho, redundância, disponibilidade, contingência e monitoramento contínuo do tráfego de acesso aos serviços digitais oferecidos pela instituição.

15.3. A solução 1 escolhida atende aos requisitos de negócio e aos requisitos tecnológicos, conforme evidenciado neste estudo. Dentre os motivos apresentados ao longo deste ETP que fundamentam a escolha da referida solução, destacam-se:

- 15.3.1. recursos capazes de enfrentar os desafios da defesa cibernética diante das atuais ameaças e ações de *malware*;
 - 15.3.2. integração e compatibilidade com os demais ativos do ambiente tecnológico interno; e
 - 15.3.3. familiaridade e domínio na operação e administração dos recursos, assim como na gestão do suporte pela equipe de TI da MB.
- 15.4. Quanto ao parcelamento da contratação, conclui-se que a solução admite parcelamento técnico, por compreender objetos distintos e autônomos, correspondentes às licenças da solução de firewall e às licenças da solução de IPS, os quais podem ser contratados separadamente sem prejuízo à compatibilidade do ambiente.

15.5. O parcelamento, nesses termos, não compromete a continuidade operacional da RECIM, uma vez que cada solução possui base instalada, licenciamento e suporte próprios. O fornecimento, contudo, dar-se-á de forma integral para cada item contratado, de modo a assegurar que as respectivas licenças sejam disponibilizadas de uma só vez e permaneçam válidas durante toda a vigência contratual.

16. Justificativa econômica da escolha da solução

16.1. O estudo apresentado neste documento considerou os melhores custos identificados, visando atender de forma eficiente e eficaz às demandas técnicas do ambiente da MB.

16.2. Os valores da solução 1 estão em conformidade com os padrões do mercado de segurança cibernética, assegurando que a MB faça um investimento eficiente em sua infraestrutura de proteção.

16.3. Além disso, em outubro de 2020 iniciou-se um investimento para troca dos equipamentos e aquisição de licenças das soluções de IPS e firewall, dos fabricantes Trellix e Cisco, respectivamente, devido ao *end-of-life* dos mesmos. Desta forma, é de suma importância preservar o investimento do hardware e licenças adquiridas.

16.4. A implantação da atual solução IPS e firewall, na MB, incluiu as fases de: homologação da solução; testes de funcionamento em rede; adaptações (customizações) para atendimento das especificidades de sigilo da MB; e implantação de sensores em Organizações Militares diversas em todo o território nacional e treinamento/capacitação de pessoal.

16.5. Os altos investimentos financeiros nos equipamentos e em capacitação de pessoal, outrora realizados em prol das atividades de defesa cibernética, permitiram que a MB, hoje, mantenha a segurança de suas redes de dados e dê continuidade às atividades e projetos de interesse da Força, possibilitando a implantação e a alteração de políticas de segurança, em sua rede de dados, com menor tempo e maior acurácia. O aperfeiçoamento técnico alcançado é fruto de persistência e constante dedicação, visto que, a introdução de uma nova tecnologia requer, conforme representação da curva de aprendizagem, maior tempo despendido para seu domínio.

16.6. Faz-se necessário considerar que, para o referido cenário, a MB precisa renovar 5 (cinco) itens, totalizando 8 (oito) unidades /licenças de atualização, suporte e garantia das soluções Trellix e Cisco, preservando assim o investimento iniciado em 2020 com a troca dos equipamentos e a capacitação da equipe.

16.7. O parcelamento da contratação decorre de aspectos técnicos relacionados à autonomia das soluções de firewall e IPS, sem prejuízo da economicidade, uma vez que preserva investimentos já realizados e evita custos adicionais de substituição tecnológica, reimplantação e capacitação.

16.8. Justificativa das exigências de qualificação técnica

As exigências de qualificação técnica previstas no Termo de Referência justificam-se pela criticidade do objeto, que envolve a renovação de licenças, subscrições, suporte, atualização e garantia de soluções responsáveis pela proteção de borda da RECIM. A interrupção, ativação incorreta, ausência de suporte válido ou indisponibilidade de atualizações de segurança pode comprometer a capacidade de detecção, prevenção e bloqueio de ameaças cibernéticas, com impacto sobre a continuidade dos serviços institucionais.

16.8.1. As exigências deverão ser objetivas, proporcionais e vinculadas à comprovação de aptidão para fornecimento, renovação, ativação ou suporte de licenças/subscrições de soluções de segurança de rede, firewall, IPS, threat prevention, malware protection, URL filtering ou objeto tecnicamente equivalente, sem impor certificações, marcas ou requisitos excessivos que restrinjam indevidamente a competitividade.

16.9. Justificativa das exigências de qualificação econômico-financeira

As exigências de qualificação econômico-financeira justificam-se pelo valor estimado da contratação, pela natureza continuada da cobertura de suporte e garantia durante a vigência contratual e pela essencialidade das soluções para a segurança cibernética da RECIM. Busca-se reduzir o risco de contratação de fornecedor sem capacidade econômico-financeira mínima para sustentar as obrigações assumidas, especialmente a emissão/renovação de licenças, a manutenção da cobertura de suporte, o atendimento a chamados e a garantia de substituição de componentes quando aplicável.

1.9.1. As exigências deverão permanecer proporcionais ao objeto e ao valor da contratação, limitando-se ao necessário para demonstrar capacidade econômica mínima, observados os parâmetros do Termo de Referência e da legislação aplicável, vedadas exigências excessivas ou desconectadas dos riscos concretos da contratação.

17. Benefícios a serem alcançados com a contratação

17.1. A manutenção das licenças para o uso da solução do firewall e IPS possibilitará à MB a manutenção da visualização global dos níveis de segurança em que se encontra a RECIM e possibilitará tomar ações imediatas para adequá-la a níveis de segurança aceitáveis, atendendo aos Objetivos Estratégicos e necessidades previstas no PDTIC.

17.2. Com a solução adotada, alguns dos benefícios a serem alcançados são: manutenção da capacidade operacional do Sistema IPS e de firewall; manutenção da capacidade de proteção da rede de dados da MB; e manutenção de políticas de segurança que contribuam para o cumprimento da LGPD; suporte e garantia do ativo de IPS em produção, minimizando possíveis indisponibilidades em caso de falha de equipamento, através do reparo ou substituição; agilidade na resolução de demandas operacionais complexas, por meio do apoio técnico especializado do fabricante.

17.3. A contratação também permitirá o alcance dos seguintes benefícios:

17.3.1. Preservar a segurança e proteção da rede interna;

- 17.3.2. Manter ativas regras e políticas de segurança;
- 17.3.3. Controle de acesso;
- 17.3.4. Monitoramento do tráfego da rede;
- 17.3.5. Visibilidade do tráfego de acesso e inspeção de pacotes;
- 17.3.6. Proteção de dados e da continuidade dos processos de negócios das ameaças sofisticadas e de ataques cibernéticos;
- 17.3.7. Mitigação de riscos;
- 17.3.8. Garantia, suporte técnico e atualização da solução; e
- 17.3.9. Integração e compatibilidade técnica com as demais soluções.

18. Providências a serem Adotadas

- 18.1. Não serão necessárias adaptações técnicas relevantes no ambiente da RECIIM para execução da solução escolhida, pois a contratação consiste na renovação de licenças, subscrições, suporte e garantia de soluções já implantadas e em operação.
- 18.2. Antes da deflagração do certame, deverão ser adotadas as seguintes providências administrativas:
 - 18.2.1. atualização do Documento de Formalização da Demanda, especialmente quanto à data pretendida para conclusão da contratação;
 - 18.2.2. juntada da Declaração de Disponibilidade Orçamentária, firmada pelo Ordenador de Despesas ou autoridade competente;
 - 18.2.3. atualização do Termo de Referência e da minuta de edital, quando aplicável, para utilização do modelo oficial mais recente indicado pela Consultoria Jurídica;
 - 18.2.4. aprovação formal dos artefatos da fase preparatória pela autoridade competente, incluindo DFD, ETP, Termo de Referência, pesquisa de preços e mapa de riscos, conforme aplicável;
 - 18.2.5. juntada aos autos do relatório de atendimento às recomendações da Consultoria Jurídica, com indicação das providências adotadas e dos documentos nos quais foram realizadas as alterações.

19. Alinhamento da contratação

19.1. Do Alinhamento entre a Contratação e o Planejamento Institucional

Em observância aos princípios da governança, da eficiência e da segregação de funções, o objeto desta contratação guarda estrita consonância com as diretrizes estratégicas e os macroprocessos da DCTIM. Esse alinhamento institucional materializa-se por meio da integração harmônica com os seguintes instrumentos de planejamento e controle:

- 19.1.1. Plano de Contratações Anual (PCA): A presente demanda encontra-se previamente cadastrada e aprovada no cronograma de contratações da Diretoria, evidenciando que a aquisição não decorre de ato intempestivo, mas sim de um planejamento prévio que visa garantir a previsibilidade orçamentária e a eficiência administrativa do certame;
- 19.1.2. Plano de Logística Sustentável (PLS): O objeto foi delineado em estrita observância às práticas de consumo consciente e critérios de sustentabilidade ambiental, social e econômica defendidos pela DCTIM, assegurando a escolha de soluções que minimizem o impacto ambiental e otimizem a eficiência energética e o ciclo de vida dos bens/serviços;
- 19.1.3 Plano de Gestão Organizacional (PGO): A contratação reflete diretamente o cumprimento das metas institucionais e operacionais estabelecidas no PGO, servindo como meio tático e de infraestrutura necessário para que a Diretoria atinja seus objetivos finalísticos, modernize suas instalações e otimize a entrega de resultados na área de Comunicações e Tecnologia da Informação da Marinha.

Assim, a convergência entre o objeto licitado e os referidos instrumentos de governança demonstra a maturidade do processo de planejamento desta Diretoria, justificando a alta relevância da contratação para a continuidade e o aperfeiçoamento das atividades administrativas e militares

20. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

20.1. Justificativa da Viabilidade

Com base nas análises técnica e econômica realizadas neste Estudo Técnico Preliminar, esta equipe de planejamento conclui pela viabilidade da contratação das licenças de atualização, suporte e garantia dos equipamentos IPS Trellix NS9500 e Firewall Cisco Firepower 2140, integrantes da solução de segurança de borda da Rede de Comunicações Integrada da Marinha (RECIM). A solução escolhida mostra-se adequada às necessidades de negócio e tecnológicas identificadas, preserva a compatibilidade com o ambiente atualmente em produção, mantém a continuidade operacional dos serviços de segurança cibernética e resguarda os investimentos anteriormente realizados pela Administração. Além disso, a contratação mostra-se economicamente vantajosa, por evitar custos adicionais com substituição tecnológica, reimplantação do ambiente e capacitação de pessoal. Diante do exposto, esta equipe declara viável o prosseguimento da contratação.

21. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

MARCUS ROGERS CAVALCANTE ANDRADE

Fiscal Requisitante

SERGIO HENRIQUE ATHAYDES FADANELLI

Integrante Técnico

DANIEL ALBERTO CAMPOS DA CUNHA VASQUES

Integrante Técnico

CAMILA DIAS DA SILVA MEDEIROS

Integrante Técnico

MARIA CARNEIRO DE REZENDE

