



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo nº 61272.001791/2023-84

Solução de Gestão de Risco Cibernético

Brasília, 24 de novembro de 2023.



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

Histórico de Revisões

Data	Versão	Descrição	Autor
22/09/2023	1.0	Elaboração da primeira versão do documento	CT(T) Munhoz
04/10/2023	1.1	Revisão de termos técnicos e cálculo do Custo Total de Propriedade (TCO)	SO-EL Bittencourt
04/10/2023	1.2	Revisão parcial do Estudo Técnico Preliminar (ETP)	CC(IM) Oliveira
05/10/2023	1.3	Revisão parcial do Estudo Técnico Preliminar (ETP)	CF Queiroz
05/10/2023	1.4	Revisão geral do Estudo Técnico Preliminar (ETP)	CMG(RM1-T) Ribeiro
23/10/2023	1.5	Revisão geral do Estudo Técnico Preliminar (ETP)	CT(T) Munhoz
23/10/2023	1.6	Revisão geral do Estudo Técnico Preliminar (ETP)	CF Queiroz
27/10/2023	1.7	Revisão geral do Estudo Técnico Preliminar (ETP)	CC(IM) Oliveira
24/11/2023	1.8	Revisão geral do Estudo Técnico Preliminar (ETP) após a emissão do PARECER n. 00416/2023/CJACM/CGU/AGU	CT(T) Munhoz



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

INTRODUÇÃO

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

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

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

1. - INFORMAÇÕES BÁSICAS

Processo Administrativo nº 61272.001791/2023-84

Categoria do Estudo Técnico Preliminar: Contratação de Serviço de Tecnologia da Informação e Comunicações (TIC).

2. - DESCRIÇÃO DA NECESSIDADE

O Centro de Inteligência da Marinha (CIM) constatou a necessidade de uma solução de gestão do risco cibernético, envolvendo as organizações e instituições que mantenham contratos, parcerias estratégicas e vínculos com a Marinha do Brasil (MB), incluindo a própria Força, a fim de que sejam identificados e mitigados os riscos cibernéticos institucionais.

A presente necessidade encontra-se alinhada com o arcabouço normativo atinente ao setor cibernético no âmbito da Defesa:

- Constituição da República Federativa do Brasil, em seu Art. 142;
- Política Nacional de Defesa (PND): Decreto 5.484, de 30 de junho de 2005;
- Estratégia Nacional de Defesa (END): Decreto nº 6.703, de 18 de dezembro de 2008;



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

- Doutrina Militar de Defesa Cibernética: Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014;
- Política Cibernética de Defesa (PCD): Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012;
- Política Nacional de Inteligência (PNI): Decreto 8.793, de 29 de junho de 2016; e
- Estratégia Nacional de Inteligência (ENI): Decreto nº 14.503, de 15 de dezembro de 2017.

A necessidade também encontra amparo com o Planejamento Estratégico 2040 da MB, atendendo aos seguintes objetivos navais (OBNAV):

- Objetivo Naval 8 (OBNAV8): Desenvolver a capacidade cibernética da MB; e
- Objetivo Naval 9 (OBNAV9): Aprimorar as Inteligências estratégica e operacional.

Alinhamento ao PDTIC 2020-2023 do CIM:

- Ação do PDTIC: Objetivo Estratégico (OE-TI 6): Fortalecer a capacidade da MB de atuar na defesa do ambiente cibernético. Metas do PDTIC associadas:
 - M7: Implementar, aprimorar e manter soluções tecnológicas informacionais;
 - M8: Implementar e aprimorar processos de tratamento de dados; e
 - M9: Fomentar as ações de Segurança da Informação e Comunicações.

2.1. Motivação/Justificativa

O Departamento de Atividades Cibernéticas do Centro de Inteligência da Marinha (CIM) produz conhecimentos de Inteligência e Contrainteligência Cibernéticas nos níveis estratégico, operacional e tático, possuindo a capacidade analítica investigatória nos níveis estratégico e operacional a partir de fontes abertas. Atualmente, o Centro não possui uma solução adequada para realizar a gestão de risco no Espaço Cibernético (ECiber) nacional, ECiber-MB e ECiber de interesse no nível tático.

Considera-se a implantação de uma solução para atender a área de Contrainteligência Cibernética, a fim de ampliar a capacidade da MB e elevar o nível de segurança da informação e das comunicações, assim como a capacidade de defesa na esfera militar, para atuação identificação e mitigação de riscos cibernéticos.

Dessa forma, justifica-se que o CIM, a fim de assessorar o processo decisório do Comandante da Marinha e da alta administração naval, necessita da aquisição de solução adequada, permitindo o aumento do escopo das avaliações realizadas pela Inteligência e Contrainteligência Cibernéticas, resultando no aumento da eficiência na avaliação de riscos, corroborando para um resultado mais eficaz dos assessoramentos e entregáveis atualmente produzidos.



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

3. - ÁREA REQUISITANTE

Área Requisitante (Unidade/Setor/Depto):

Centro de Inteligência da Marinha
Departamento de Atividades Cibernéticas
Divisão de Contrainteligência Cibernética

Responsável pela demanda:

CT(T) Mauricio Fulginiti Olivaes Munhoz

Matrícula/SIAPE: 09.0022.01

E-mail: munhoz.mauricio@marinha.mil.br

Telefone: (61) 3429-1635

4. - DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

Identificação das necessidades de negócio

- 1 Incremento na consciência situacional sobre o ECiber nacional, ECiber-MB e ECiber de interesse;
- 2 Aumento da eficácia na coleta de dados de Contrainteligência Cibernética;
- 3 Mapeamento de vulnerabilidades da MB, de parceiros estratégicos e de organizações de interesse;
- 4 Potencial constatação da existência ameaças cibernéticas institucionais;
- 5 Identificação das atividades maliciosas na *Deep Web* e *Dark Web* que envolvam a própria MB, os parceiros estratégicos e as organizações de interesse com potencial de impacto no ECiber-MB;
- 6 Acompanhamento baseado na Inteligência de Ameaças Cibernéticas no ECiber nacional, ECiber-MB e ECiber de interesse; e
- 7 Identificação e categorização de diversos aspectos a compor o risco cibernético de uma organização de interesse.



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- 1 A solução deverá exibir diferentes características das organizações de interesse, sempre que a coleta de dados em fontes abertas estruturadas ou não permitirem, tais como:
 - Exposição às vulnerabilidades não corrigidas (CVE, *zero-day*, ativos de rede com versões obsoletas, soluções de TIC com versões obsoletas);
 - Histórico da ocorrência de incidentes cibernéticos nos últimos 12 meses;
 - Histórico do vazamento de dados sigilosos e credenciais de acesso – ex.: e-mails corporativos, sistemas internos e serviços on-line;
 - Relatar a existência de recursos e ativos de Defesa e Proteção Cibernética tais como: *Endpoint Security*, *Antivirus*, *Firewall*, *XDR*, *IPS/IDS*, sempre que a detecção desses recursos for possível;
 - Avaliação do estado e exposição do DNS no domínio principal e subdomínios;
 - Indicador do nível de segurança da rede de dados da organização, em caráter de projeção ou preditivo;
 - Exposição da organização alvo às técnicas de engenharia social e de dados que sejam entendidos como uma vulnerabilidade de segurança organizacional;
 - Análise dos endereços IP de borda da organização quanto à exposição, presença em *blacklists*, observação de tráfegos anômalos e comunicação com os endereços IP de atores de ameaça cibernética conhecidos;
 - Quando os dados coletados permitirem, apresentar um indicador do nível de governança em TIC;
 - Exibir dados sobre a segurança das aplicações, informações e serviços disponibilizados por meio dos sites da organização;
 - Exposição na *Deep Web* e *Dark Web*: presença de dados sensíveis da organização em fóruns *hacker*;
 - Exibir dados sobre infecções por *malwares* atrelados às *botnets*;
 - Exibir dados sobre propagação de *spam*;
 - Existência de dados em servidores de *malware* (*ransomware*, *wiper*, *trojan*, *RAT*) que possam levar à inferência de infecção da organização de interesse;
 - Existência de comunicações não solicitadas externamente, como por exemplo, *port-scan* originários da infraestrutura da própria organização de interesse;
 - Exibir dados sobre sistemas executando aplicativos potencialmente



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- indesejados, como por exemplo: *adware*; e
 - Exibir a infecção de *malwares* específicos por nome, além de fornecer detalhes e instruções de correção.
- 2 As coletas de dados não intrusivas do espaço cibernético da organização de interesse, preferencialmente, cobrirão os seguintes aspectos tecnológicos em caráter de detalhamento:
- Endereços IP da borda da rede (visibilidade para a Internet):
 - Portas de serviço ou aplicação abertas sem necessidade;
 - Serviço de *proxy* anônimo;
 - Existência de indicadores de ataque, ou do inglês *Indicator of Attack* (IoA);
 - Existência de indicadores de comprometimento, ou do inglês *Indicator of Compromise* (IoC);
 - Vulnerabilidades em certificados SSL/TLS (certificados expirados, autoassinados, revogados, com vida útil com tempo muito longo, emprego de algoritmo inadequado);
 - Presença de *malwares* (*ransomwares*, *wipers*, *bots*, *Remote Access Trojans* - RAT) enviando sinal de *beacon* ao servidor de comando e controle (C2) de ator adverso;
 - Presença de nós da rede TOR;
 - Presença de servidores de compartilhamento de arquivos *peer-to-peer* associados aos *torrents*;
 - Presença de servidores de C2 dentro da rede de dados da organização;
 - Vazamento de dados:
 - Exposição de credenciais de acesso de e-mails corporativos e sistemas institucionais;
 - Histórico de credenciais de acesso vazadas nos últimos 12 meses;
 - Temas relacionados ao *Domain Name Server* (DNS):
 - Existência de acesso irrestrito às configurações dos registros DNS;
 - Existência de registros inválidos nos DNS utilizados pela organização;
 - Presença do serviço de OpenDNS competindo com os redirecionamentos dos DNS organizacionais;
 - Existência de falhas ou vulnerabilidades relacionados à implementação



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- de DNSSEC;
- Segurança da rede de dados da organização:
 - Detecção da presença do serviço de *Elasticsearch* de forma ostensiva na rede de dados;
 - Exposição de serviço FTP exposto à Internet;
 - Exposição de serviços IMAP/POP3 à Internet de maneira insegura;
 - Detecção de redes industriais/operacionais que hospedam sistemas ICS/SCADA expostos à Internet;
 - Detecção de impressoras, câmeras IP e de ativos de segurança organizacional presentes na rede de dados da organização expostos à Internet;
 - Exposição de serviços como Samba (protocolo SMB), LDAP ou *Active Directory* à Internet;
 - Exposição do serviço e/ou das respectivas interfaces de acesso aos bancos de dados da organização (*Microsoft SQL Server*, *Oracle Database*, *MySQL*, *PostGre*, *MongoDB* e similares);
- Questões relacionadas às ofensivas de *hackers*:
 - Domínio(s), subdomínio(s) e endereço(s) IP públicos da organização sendo relacionados em investidas *hacker* nos últimos 12 meses;
 - Domínio(s) e subdomínio(s) sendo relacionados como vítimas em casos de *ransomware*, *wiper* ou *RAT* nos últimos 12 meses;
- *Patches* de correção e versão corrente dos ativos informacionais:
 - Ativos informacionais no fim da vida útil ou considerados obsoletos;
 - Observação de vulnerabilidades relacionadas aos *Common Vulnerabilities and Exposures* (CVE) de alta, média e baixa criticidade;
 - Observação de vulnerabilidades do tipo *zero-day* conhecidas nas versões dos ativos informacionais em uso;
- Engenharia social:
 - Exposição de dados de pessoal em caráter corrente;
 - Existência de vazamentos de dados sensíveis da organização em bancos de dados nos fóruns *hacker*;
 - Histórico de exposição de dados de pessoal nos últimos 12 meses;
- Segurança das aplicações (*web*):



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- Gestão inadequada de configuração dos servidores de hospedagem *web*;
 - Padrão de redirecionamento em protocolos HTTP/HTTPS realizados de forma insegura;
 - Configurações incorretas ou vulneráveis na utilização dos protocolos SSL e TLS;
 - Gerenciadores de conteúdo configurados de maneira não segura e/ou com vulnerabilidades conhecidas.
- 3 A solução deverá fornecer uma visão geral das organizações monitoradas, com indicadores de risco cibernético e seus vetores avaliados no ECiber.
- 4 A solução deverá permitir a troca dinâmica das organizações observadas pela ferramenta, permitindo à Administração Naval a escolha das organizações monitoradas, permitindo que até 10 organizações sejam simultaneamente monitoradas mensalmente.
- 5 A solução deverá permitir a elaboração de comparativos do nível de risco cibernético com outras organizações de interesse (Ex.: entre as marinhas do entorno estratégico brasileiro, entre as Forças Armadas de outros países, entre as organizações do mesmo setor ou de porte equivalente).
- 6 As descobertas de dados de Contraineligência Cibernética devem ser detectadas por meio de fonte de dados ativa, passiva e de terceiros, não intrusivas. Os métodos ativos de coleta de dados devem incluir sensores que rastreiam a Internet em busca de vulnerabilidades de segurança que podem ser exploradas por atores adversos. Os métodos de dados passivos, como buracos (*sinkhole*), *honeypots* e coleta de dados de trocas de publicidade, bem como fontes de terceiros devem completar a coleta para fornecer uma imagem abrangente dos controles de segurança das empresas que estão sendo monitoradas.
- 7 A plataforma deve incluir, no mínimo, os principais fornecedores associados à organização alvo e poder catalogar rapidamente novos fornecedores que podem ou não ser monitorados no momento, descrevendo a cobertura atual (empresas, domínios, subdomínios e endereços IP).
- 8 A solução deve fornecer recursos analíticos profundos, incluindo a capacidade de entender o desempenho relativo da organização no contexto de pares (organizações de natureza ou porte similar), fornecendo uma profunda visão *forense* para analisar possíveis problemas em sua infraestrutura, além da previsão de modificações e simulações de alteração do risco cibernético da organização de interesse.



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- 9 A funcionalidade de gestão do risco cibernético propriamente dito deve ter, no mínimo, as seguintes características:
- Atualizações diárias, para cada entidade monitorada;
 - Dados de histórico diário até os 12 meses anteriores, desde que a empresa esteja monitorada na solução;
 - O *scan* automático das vulnerabilidades deve ocorrer até o máximo de 30 dias;
 - Cada vetor de risco que compõem a classificação deve ser avaliado individualmente, com uma métrica própria para atribuição do nível de risco;
 - Preferencialmente, a correlação entre vazamentos de dados e a avaliação do risco cibernético poderá ser validada independentemente por meio de um terceiro;
 - Todos os eventos que impactam a avaliação do risco devem ser apoiados com evidência objetiva, verificável e que também permita uma ação nos mesmos e a pontuação do impacto na métrica visível;
 - Visualização total da pegada digital, do inglês *digital footprint*, composta por endereços IP, domínios e subdomínios, para todas as organizações monitoradas, sem a necessidade de autorização da organização alvo, com as respectivas evidências para cada vetor;
 - *Scan* de todos os IP públicos quer da própria entidade, quer de todos os terceiros e/ou fornecedores, no máximo a cada 30 dias com a data de validação na solução;
 - Deve ser nativo da solução o envio e a recepção de questionários de segurança customizados, preferencialmente, em português do Brasil, sendo personalizável sobre qualquer questionamento de segurança ou não;
 - Preferencialmente, permitir a criação de métricas customizadas pela *digital footprint* e/ou localização dos IP quer para a própria organização, bem como para qualquer terceiro a monitorar;
 - Relatórios resumidos e detalhados disponibilizados na solução, preferencialmente, em português do Brasil. Caso não seja possível, os relatórios deverão ser disponibilizados em Inglês;
 - Sobre as vulnerabilidades ou eventos detectados na solução e identificadas como remediadas pelo usuário e aceites pela solução como tal (com exceção da cadência de patches): o impacto das mesmas deverá refletir-se na métrica de avaliação de risco cibernético em até 10 dias;



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- A possibilidade de estabelecer ações automáticas sobre alguma nova vulnerabilidade, evento ou incidente, não afeta alguma entidade e/ou métrica de avaliação de risco cibernético, como no caso de envio automático de relatórios resumidos e detalhados para os usuários da plataforma;
 - A metodologia tem de ser pública e disponibilizada na internet, bem como os dados devem ser fornecidos a qualquer usuário ou empresa que os solicite; e
 - Deve possuir a funcionalidade de visualização das entidades monitoradas em nível geral (*watchlist*) com informações sobre sua métrica e a variação desse nos últimos 30 dias, sem que isso impacte a quantidade de entidades monitoradas em nível profundo.
- 10 A solução deve ser capaz de mostrar rapidamente quais fornecedores apresentam incidentes significativos em seu ECiber.
- 11 A solução deve ser capaz de mostrar rapidamente quais fornecedores têm vulnerabilidades e quais são elas.
- 12 A solução deve oferecer às organizações-alvo a capacidade de ver sua avaliação de risco cibernético gratuitamente.
- 13 A solução tem de demonstrar com transparência a porcentagem de impacto que determinada vulnerabilidade tem na métrica tanto da organização alvo, como de qualquer terceiro que se esteja a monitorar.
- 14 A desenvolvedora da solução deverá ser considerada líder por, pelo menos, uma empresa de análise independente como a *Forrester* ou a *Gartner*.
- 15 A solução deverá possibilitar a personalização de um painel por endereços IP, domínios, ou localização geográfica, tanto para a MB, como para qualquer organização que se esteja a monitorar. Essa opção deve ser realizada pela MB sem a necessidade de suporte.
- 16 A *digital footprint* de todas as organizações mapeadas na solução tem de ser atualizadas automaticamente no mínimo a cada 30 dias, para validação da *digital footprint*.
- 17 A solução deverá ter um mínimo de 10.000.000 de empresas, entidades e organizações já mapeadas na plataforma e disponível para monitorização imediata pelo usuário.
- 18 A solução para mapeamento de uma nova empresa, organização ou entidade, que



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- ainda não exista no catálogo de empresas mapeadas, não pode levar mais de 24 horas para que esse novo alvo de interesse fique disponível em caráter inicial no portal.
- 19** A MB terá acesso à visualização de toda a *digital footprint*, entenda-se por endereços IP, domínios e subdomínios de qualquer organização que se deseje monitorar, sem que seja necessária a autorização desse alvo para tal.
- 20** A MB observará os dados *forenses* detalhados dos eventos detectados de qualquer organização que necessite monitorar.
- 21** Toda e qualquer vulnerabilidade presente na avaliação das organizações de interesse deverá ter visível qual a porcentagem que essa vulnerabilidade afetou ou está a afetar a avaliação do risco cibernético.
- 22** A solução deve oferecer um processo totalmente interativo para ajustar as coletas digitais das empresas na plataforma, com a possibilidade de remover endereços IP que podem não ser necessários e adicionar os endereços IP de interesse.
- 23** As unidades, subsidiárias e fusões de uma organização de interesse poderão ser agrupadas em um único painel de vetores. Também deve permitir ao usuário gerar painéis personalizados tanto para a MB, como para qualquer organização monitorada.
- 24** Deverão ser disponibilizados relatórios diversificados sobre os dados coletados e apresentados pela solução, sendo oferecidos, pelo menos, em formato PDF para *download*. Preferencialmente, o idioma dos relatórios será o português do Brasil. Quando não houver possibilidade do idioma preferencial, deverão ser fornecidos em Inglês. Os tipos de relatórios fornecidos serão:
- Relatório resumido, contendo a avaliação do risco cibernético da organização de interesse e os vetores que compõe essa avaliação;
 - Relatório dos eventos e/ou vulnerabilidades encontrados das organizações monitoradas;
 - Relatório detalhado com dados *forense*, com visibilidade no nível do(s) domínio(s), subdomínio(s) e endereço(s) IP afetado(s), seja nos relatórios gerados para a MB, como nos relatórios gerados para avaliação do risco cibernético de qualquer organização alvo;
 - Relatórios de nível de problemas e eventos potencialmente prejudiciais ao ECiber de interesse;



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- Relatórios de comparação do risco cibernético e seus vetores entre as organizações monitoradas; e
- Relatórios customizados de forma *ad-hoc*, com a possibilidade do usuário selecionar os dados da organização de interesse conforme for conveniente.

25 A solução deverá conter dados de tendências históricas e classificações do risco cibernético das organizações de interesse, apresentado o nível de detalhamento apresentado, a fim de demonstrar o progresso ou declínio de uma organização ao longo do tempo.

26 A plataforma deverá incluir análise de ameaças cibernéticas, preferencialmente indicando a criticidade, quando houver suspeita de infecção, além de instruções de remoção da ameaça.

27 O modelo de pontuação deve ser determinístico, ou seja, uma organização alvo poderá ver no nível do problema como sua pontuação, sobre como ela é impactada positiva ou negativamente por um problema específico na avaliação do risco cibernético.

28 O tempo de resposta do suporte técnico deverá ser de, no máximo, 24 horas úteis.

29 A solução deve fornecer uma API REST completa. A API deve estar totalmente acessível na plataforma e incluída na presente aquisição do serviço. Preferencialmente, ter integrações prontas para uso com as principais ferramentas empregadas na gestão de riscos, tais como: *Ticket Management, SIEM, Service Now - VRM, Service Now - IT SM, RSA Archer GRC, Splunk, SAI Global, IBM Qradar, LockPath, ProcessUnity, Rsam, Venminder, ORACLE CASB, Glavaníze, Egan-Jones, Aravo, RMS, Third Party Trust, Proactive Risk, NRI Secure - Secure SketCH, One Trust Vendorpedia, DFLabsk SecurityGate IO/OT RMk CrowdStrikek Palo Alto Cortex XSOArk Teamsk Slack e Jira.*

30 Preferencialmente, ter uma solução nativa para envio e recepção de questionários baseados em *frameworks* como GDPR, ISO, NIST, HIPAA, TISAX, CSA, PCI bem como a possibilidade do usuário customizar os seus próprios questionários em português do Brasil para verificação do atendimento à LGPD e à BACEN 4658;

31 A solução deverá mostrar as informações coletadas dos atores de ameaça cibernéticos, os quais potencialmente estariam a explorar o ECiber de interesse. Além da suposta presença de atores adversos, deverá mostrar se eles estão explorando vulnerabilidades em uma organização monitorada e, também, se existem vulnerabilidades que não estão sendo explorada, mas que poderia vir a ser



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Identificação das necessidades tecnológicas

- alvo dos atores de ameaça.
- 32 A solução deverá basear-se os indicadores em *frameworks* de segurança consolidados internacionalmente pela comunidade de TIC;

Demais requisitos necessários e suficientes à escolha da solução de TIC

- 1 A solução deverá ser disponibilizada na modalidade de software como serviço, ou do inglês “*Software-as-a-Service*” (SaaS), permitindo o acesso da MB via Web, de maneira a não depender de hospedagem dos serviços no parque computacional de Tecnologia da Informação e Comunicações (TIC) da MB.
- 2 A disponibilidade da solução deverá ser maior que 93,4% em 12 meses.
- 3 As organizações selecionadas para serem acompanhadas pela solução deverão ser de caráter sigiloso, não sendo reveladas a terceiros.
- 4 A solução deverá permitir o emprego de senhas seguras com mais de 12 caracteres, com mecanismo de recuperação de senha em caso de esquecimento pelo usuário.
- 5 A solução deverá ser compatível com os navegadores Google Chrome, Microsoft Edge e Mozilla Firefox nas suas versões mais atuais.
- 6 A interface da solução deverá ser apresentada no(s) idioma(s) português do Brasil e/ou inglês.
- 7 A solução deverá ser de fácil uso, com uma interface intuitiva e com a possibilidade de serem criados e administrados múltiplos usuários para uso da MB.
- 8 A plataforma deverá permitir o *download* todos os dados de descobertas com os endereços IP mostrados, domínios, subdomínios, vulnerabilidades e alertas para que se possa corrigir esses itens de maneira *off-line*, tanto da infraestrutura da MB, como na de qualquer organização que se esteja monitorando.
- 9 É preferencial que a solução disponha de recurso de auxílio à utilização, tal como tutoriais, manuais e/ou instrução ministrada nas modalidades presencial ou à distância por representante para início do seu uso.
- 10 A solução deverá dispor de um meio para apresentar a metodologia utilizada na avaliação do risco cibernético de maneira pública, a fim de permitir o entendimento pela Administração Naval e das organizações monitoradas dos critérios empregados em cada vetor.



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

- 11 A MB poderá solicitar a alteração das credenciais de acesso dos usuários da plataforma conforme a sua necessidade.
- 12 Preferencialmente, a plataforma contemplará uma tela inicial com informações consolidadas para visualização das organizações monitoradas e alertas cadastrados.

Preferencialmente, a autenticação do usuário na plataforma contará com duplo fator de autenticação (2FA), oferecendo uma das opções: e-mail ou “One Time Password” (OTP). Caso a opção de 2FA seja oferecida por meio de SMS, esta funcionalidade deverá ser implementada pela CONTRATADA e o efetivo envio de mensagens deverá ocorrer sem qualquer custo adicional para a MB.
- 13
- 14 A plataforma deverá exibir todos os relatórios e gráficos em painéis de fácil leitura (*dashboards*).
- 15 Preferencialmente, ter as informações apresentadas na plataforma disponíveis para o *download* em diferentes formatos, como: HTML, PDF ou CSV.

5. – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

A solução abrange a prestação do serviço de coleta e integração de dados para gestão do risco cibernético do ECiber de interesse, consolidados e processados segundo uma metodologia própria de risco cibernético definida pelo fornecedor.

O modelo conceitual que melhor ilustra a solução a ser obtida seria de um sistema de avaliação de risco cibernético integrado, apresentando os dados de forma textual e gráfica, no que couber, permitindo a extração de relatórios das análises.

A solução deverá ser disponibilizada no formato SaaS, sendo que sua utilização se dará por meio de um portal acessível pela *Web*, com credenciais fornecidas à MB, de maneira que somente múltiplos usuários terão acesso simultâneo à solução. A duração prevista do acesso será de 12 (doze) meses a contar da assinatura do contrato.

Pretende-se, ainda, que a solução seja acompanhada dos seguintes serviços:

- Treinamento, e/ou a disponibilidade de um *workshop*, e/ou tutorial de utilização com manual por escrito e apresentações gravadas em vídeos, suficientes ao bom uso das capacidades da solução; em até 2 semanas do recebimento do pagamento e
- Suporte técnico provido em português do Brasil, na modalidade à distância.



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

6. - ANÁLISE DE SOLUÇÕES

Soluções que trabalhem com a avaliação de risco, ou mais especificamente, gestão do risco cibernético no tocante ao ECiber de interesse, tem surgido no mercado privado. Em uma pesquisa na *web*, foram encontradas diversas alternativas que variam no desempenho, alcance dos dados coletados, metodologia empregada na análise, quesitos identificados para compor uma nota geral da instituição, entre outras funcionalidades específicas relacionadas ao foco de cada solução.

A área de Contrainteligência Cibernética na MB possui particularidades que não são comuns aos demais setores da TIC, de maneira que ferramentas e soluções integradas específicas, que atendam ao arcabouço normativo do setor de Inteligência e às necessidades internas do CIM, se fazem necessárias.

Não foram observadas soluções equivalentes no que é concebido como software público brasileiro.

Não serão necessárias adequações do ambiente de TIC da MB, dado que o serviço buscado deverá ser prestado por meio de acesso *web*, sendo uma prática comum do setor essa modalidade.

6.1. - IDENTIFICAÇÃO DAS SOLUÇÕES

6.1.1. - SOLUÇÃO A: LOCAÇÃO DOS ATIVOS DE TIC PARA A EXECUÇÃO DO SERVIÇO

Dadas as especificidades de uma solução de gestão de risco cibernético, envolvendo um mercado restrito de fornecedores e utilizadores, a modalidade vigente para o setor cibernético, de provimento da solução no formato SaaS, não contempla o aluguel dos ativos para a execução do serviço. Um detalhamento das premissas e aspectos legais envolvidas para esta solução está disponível no item 8.3.1.

6.1.2. - SOLUÇÃO B: AQUISIÇÃO DA ESTRUTURA DE TIC (HARDWARES) PARA A HOSPEDAGEM DA SOLUÇÃO DE GESTÃO DE RISCO CIBERNÉTICO

Considerando a restrição orçamentária da Marinha do Brasil, dada a necessidade de aquisição de toda uma infraestrutura de hospedagem local do serviço, além de ser necessário comprar uma solução de gestão de risco cibernético (software), de maneira proprietária, para utilizá-la como um serviço sendo executado localmente, torna-se inviável pelo custo e pela não disponibilidade no mercado de aquisição do software nesta modalidade. Um memorial descritivo sobre esta solução e os respectivos cálculos dos valores envolvidos está disponível no item 8.3.2.



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

6.1.3. - SOLUÇÃO C: CONTRATAÇÃO NA MODALIDADE “SOFTWARE COMO SERVIÇO” (SAAS – “SOFTWARE-AS-A-SERVICE”)

As principais soluções de gestão de risco cibernético, de natureza similar, disponíveis no mercado, que potencialmente atenderiam à presente necessidade de contratação do CIM, considerando as características em comum, serão demonstradas mais adiante na Tabela 1. Aquelas que estariam com forte adesão na utilização por grandes empresas, sendo bem avaliadas nos sites especializados, recebendo comentários favoráveis ao serviço prestado foram identificadas a seguir:

- *BitSight Security Ratings Platform* ⁽¹⁾ (<https://www.bitsight.com>)
- *SecurityScorecard Ratings* ⁽²⁾ (<https://securityscorecard.com/>)
- *UPGuard Ratings* ⁽³⁾ (<https://www.upguard.com/product/security-ratings>)
- *OneTrust Third-Party Risk Management Ratings* ⁽⁴⁾ (<https://www.onetrust.com/>)
- *RiskRecon Ratings* ⁽⁵⁾ (<https://www.riskrecon.com/>)

Id	Descrição da solução de gestão de risco cibernético
1	<i>BitSight Security Ratings Platform</i> ⁽¹⁾ (https://www.bitsight.com) A Bitsight opera com o gerenciamento de risco cibernético, com a proposta de transformar a forma como as empresas gerenciam exposição, desempenho e risco para si mesmas e para terceiros, por meio de sua plataforma web. Empresas de todos os tamanhos e setores tem recorrido à Bitsight para expandir ecossistemas distribuídos sem se preocupar com superfícies de ataque expandidas. Para acelerar a transformação sem acelerar os problemas financeiros. Para adicionar fornecedores sem adicionar suas vulnerabilidades. E fazer com que todos trabalhem de forma sinérgica no setor de risco cibernético.
2	<i>SecurityScorecard Ratings</i> ⁽²⁾ (https://securityscorecard.com/) A SecurityScorecard é uma empresa de segurança da informação que classifica as posturas de segurança cibernética de entidades corporativas por meio da conclusão de análises pontuadas de sinais de inteligência de ameaças cibernéticas para fins de gerenciamento de terceiros e gestão de risco cibernético. As funcionalidades são oferecidas como um serviço de sua plataforma web.
3	<i>UPGuard Ratings</i> ⁽³⁾ (https://www.upguard.com/product/security-ratings) Com possibilidade de visibilidade da superfície de ataque e dos riscos de terceiros, oferece a gestão de risco cibernético como algo prioritário. A solução proprietária é disponibilizada por meio de uma plataforma web multifuncional. Gerenciamento de risco de terceiros: monitoramento contínuo de fornecedores, automatização dos questionários de segurança e proposta de redução do risco de terceiros.



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Id	Descrição da solução de gestão de risco cibernético
4	OneTrust Third-Party Risk Management Ratings ⁽⁴⁾ (https://www.onetrust.com/) Plataforma de serviços <i>online</i> para avaliação de parceiros de negócio em diversos aspectos, sendo a avaliação da vertente cibernética uma delas. Dispõe de um fluxo de dados significativo, juntamente com preocupações éticas e regulatórias crescentes. A denominada <i>Trust Intelligence Platform</i> ajuda a resolver esses desafios, ao mesmo tempo em que simplifica as operações com automação e orientação regulatória integrada.
5	RiskRecon Ratings ⁽⁵⁾ (https://www.riskrecon.com/) A plataforma <i>online</i> da RiskRecon avalia a qualidade do desempenho de risco de segurança cibernética de uma organização usando uma escala rotulada de A a F e uma escala numérica de 0,0 a 10. A classificação é baseada nas taxas e na prioridade de risco dos problemas presentes no ambiente, conforme observado pelos algoritmos passivos de avaliação de risco na plataforma.

Tabela 1 – descrição das principais soluções similares identificadas, segundo pesquisa no portal Gartner.com em FEV2023.

6.1.4. - SOLUÇÃO D: DESENVOLVIMENTO DE UM SISTEMA SIMILAR, PELA PRÓPRIA MB, QUE ATENDAS AS NECESSIDADES ELENCADAS NESTE ETP

Esta solução foi considerada inviável, devido à falta de orçamento, disponibilidade de pessoal técnico dedicado e conhecimento técnico na MB suficientes para conceber e manter uma solução de gestão de risco cibernético de maneira longa e adequada ao propósito de sua utilização.

6.2. - ANÁLISE COMPARATIVA DE SOLUÇÕES

Cabe ressaltar que o comparativo disposto a seguir (Tabela 2) foi obtido com base nos dados fornecidos de forma aberta e gratuita pela consulta ao portal *Gartner Peer Insights Community* (disponível em: www.gartner.com). A organização é uma comunidade livre com elevado nível de confiabilidade, com dados fornecedores para auxílio de decisores da área de Tecnologia da Informação e Comunicações (TIC), a fim do compartilhamento de conhecimentos de soluções de mercado em tempo real.

Contando com mais de 20.000 entidades analisadas, a plataforma da *Gartner* oferece, semanalmente, relatórios de *benchmark* de soluções, pesquisas e relatórios de *insights*, avaliando cada fornecedor em cerca de 21 itens, com o fito de obter dados comparativos de forma rápida e eficaz.



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

Solução/ Característica	BitSight ⁽¹⁾	Security Scorecard ⁽²⁾	UpGuard ⁽³⁾	OneTrust ⁽⁴⁾	RiskRecon ⁽⁵⁾
Acesso e controles do usuário	4,5	4,4	4,6	4,4	3,5
Estimativas/Validação/ Controles de monitoramento	4,4	4,4	4,4	4,4	4,3
Avaliações	4,4	4,4	4,2	4,3	4,2
Facilidade de configuração	4,2	4,1	4,4	4,3	3,5
Conexões e integração	4,3	4,3	4,1	4,2	4,0
Histórico e relatórios	4,5	4,4	4,3	4,3	4,5
Gerenciamento de exceções	4,2	4,1	4,2	4,2	5,0
Histórico	4,3	4,4	4,5	4,4	5,0
Gerenciamento e contingências para exceções	4,2	4,1	4,3	4,2	4,3
Usabilidade e acesso	4,5	4,5	4,4	4,4	4,4
Gerenciamento de perfis	4,4	4,3	4,4	4,4	4,0
Fluxo de trabalho e colaboração	4,3	4,2	4,3	4,3	4,1
Flexibilidade de negociação de preço	4,2	4,4	4,5	4,5	4,6
Habilidade de compreender as necessidades da contratante	4,4	4,6	4,7	4,4	4,6
Facilidade de implementação	4,7	4,8	4,7	4,5	4,8
Qualidade do treinamento ao usuário	4,4	4,5	4,5	4,3	4,3
Facilidade de integração utilizando as API e ferramentas padronizadas	4,2	4,3	4,5	4,3	4,2
Disponibilidade de recursos de terceiros	4,2	4,3	4,4	4,2	4,4
Pontualidade na resposta do fornecedor	4,6	4,7	4,7	4,6	4,6
Qualidade do suporte técnico	4,5	4,7	4,6	4,6	4,7
Qualidade dos usuários pertencentes à comunidade	4,2	4,5	4,5	4,2	4,5
Avaliação geral da solução	4,5	4,5	4,4	4,4	4,5

Tabela 2 – Comparativo por características e funcionalidades das principais soluções similares disponíveis no mercado (consulta efetuada em FEV2023).

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2		X	
	Solução 3		X	
	Solução 4		X	
	Solução 5		X	
A Solução está disponível no Portal do Software Público Brasileiro?	Solução 1		X	
	Solução 2		X	



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

Requisito	Solução	Sim	Não	Não se Aplica
(quando se tratar de software)	Solução 3		X	
	Solução 4		X	
	Solução 5		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
	Solução 4		X	
	Solução 5		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
	Solução 5			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
	Solução 5			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
	Solução 5			X

Tabela 3 – Quadro comparativo das plataformas de mercado diante de requisitos comuns à contratação de soluções de TIC para a administração pública.

Não foram observadas equivalências ou proximidades com as soluções disponíveis no Catálogo de Soluções de TIC, definidas pelo Órgão Central do SISP, no âmbito do processo de gestão estratégica das contratações de soluções baseadas em software de uso disseminado previsto no § 2º do art. 43 da Lei nº 14.133, de 2022 (disponível em: <https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic>).

Não se aplicam à solução pretendida as políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil.



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

7. - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

As soluções A, B e D foram consideradas inviáveis, conforme o descrito nos itens 6.1.1, 6.1.2 e 6.1.4, respectivamente.

8. - ANÁLISE COMPARATIVA DE CUSTOS (TCO)

8.1. - CUSTO TOTAL DE PROPRIEDADE (TCO) PARA CONTRATAÇÕES DAS SOLUÇÕES PROPOSTAS:

A presente seção registra a comparação de Custos Totais de Propriedade para as soluções técnica e funcionalmente viáveis, nos termos da IN SGD-ME nº 01/2019, em seu inciso III do art. 11, assumem-se premissas para se aproximar ao máximo da realidade dos diferentes órgãos que registraram a demanda.

8.2. - CUSTOS ADMINISTRATIVOS DAS SOLUÇÕES:

Tendo como base a IN SGD-ME nº 01/2019, o Custo Total de Propriedade é obtido por meio da composição dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução contratada e suas respectivas manutenções.

Para o presente documento realizou-se a estimativa de custo administrativo inerente a cada solução abrangendo todo o seu ciclo de vida, a saber:

- 1) Planejamento da Contratação e Realização da Licitação;
- 2) Gerenciamento da Ata de Registro e Preço;
- 3) Fiscalização e Gestão do Contrato; e
- 4) Renovação do Contrato.

Para o ponto do Planejamento da Contratação e Realização da Licitação acatou-se como referência para o cálculo do custo administrativo da dispensa de licitação (ver: Governo Federal, Contrato N°. 06/ 47-2825, Relatório Técnico 12. Brasília: FIA, IDSSCHEER Sundfeld advogados, 2007, 2007, citado pela nota técnica nº 1081/2017/CGPLAG/DG/SFC/CGU, disponível em: <http://www.planejamento.gov.br/assuntos/servidores/painel-estatistico-de-pessoal>).

Foram levantados as remunerações inicial e final para todos os postos e graduações dos militares da Marinha do Brasil, disponível em: https://www.marinha.mil.br/sites/default/files/anexo_ii_-_remuneracao_e_subsidios_de_cargos_efetivos_-_postos_e_graduacoes_-_dez2020.pdf



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

8.2.1. - ELABORAÇÃO E ACOMPANHAMENTO DOS DOCUMENTOS DO PROCESSO LICITATÓRIO:

A fim de contextualizar todo o conjunto de elementos que envolvem o cálculo dos custos, segue uma breve introdução naquilo que tange a fase da elaboração dos documentos do processo e os custos envolvidos.

Segundo estudo, realizado pelo Instituto Negócios Públicos em 2018, foram estimados os custos médios dos processos licitatórios considerando todas as fases do processo. A análise do custo médio de uma licitação foi realizada por meio dos gastos em cada fase do processo, conforme a descrição a seguir:

- 1) Identificação da necessidade de bens ou serviços: R\$ 1.182,18;
- 2) Análise e aprovação da aquisição: R\$ 810,85;
- 3) Realização de pesquisa de mercado de valores e quantidades: R\$ 2.908,81;
- 4) Determinação da modalidade e projeto básico ou termo de referência: R\$ 2.373,41;
- 5) Elaboração de minuta do edital, contrato e publicação: R\$ 4.456,81;
- 6) Abertura das propostas e habilitação dos interessados em ato público: R\$ 1.667,91; e
- 7) Verificação nas conformidades com o edital, adjudicação e homologação e publicação do resultado: R\$ 2.772,99.

Ressalte-se que os valores médios apresentados no estudo do Instituto Negócios Públicos não distinguem o tipo de procedimento licitatório e, nesse sentido, não foi considerado o fato de que, ao menos em tese, o tempo de realização de uma dispensa seria menor, o que acarretaria custos menores.

Em uma visão conservadora, não foram apropriados no valor acima referido os custos das demais fases, que também estão presentes no processo de dispensa de licitação, nem tão pouco foram associados os valores do homem-hora (HH) dos órgãos gestores, neste caso a MB.

Para fins de uma base de cálculo, utilizou-se os valores apresentados acima e a eles foi somado o custo de HH referentes a 3 (três) servidores públicos de nível superior e 3 (três) servidores públicos de nível médio por um período de 20 horas. O resultado foi de R\$ 52.612,80 (cinquenta e dois mil, seiscentos e doze reais e oitenta centavos).

8.2.2. - ÍNDICE DE CUSTO DA TECNOLOGIA DA INFORMAÇÃO (ICTI) - JUN2023:

O Índice de Custos da Tecnologia da Informação (ICTI) tem por objetivo captar a evolução específica dos custos efetivos da área de TI. Os custos do governo federal tem como base os índices gerais, os quais apenas orientam as tomadas de decisões visando evitar prejuízos indevidos ao erário ou às empresas fornecedoras de serviços de TI.



MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA

O Índice de Custo da Tecnologia da Informação (ICTI), calculado pelo Instituto de Pesquisa Econômica Aplicada (Ipea), apresentou taxa de variação de -0,3% em junho de 2023, situando-se 0,04 ponto percentual (p.p.) acima da taxa registrada no mês anterior. Na comparação com o mesmo mês de 2022, a variação foi 1 p.p. menor (Tabela 4).

ICTI versus índices amplos de preços de outras fontes (jun./2023)

(Em %)

	ICTI	IPCA	IGP-M	IPA-EP
	Ipea	IBGE	FGV	FGV
Junho de 2023	-0,30	-0,08	-1,93	-2,13
Junho de 2022	0,70	0,67	0,59	0,44
Acumulado em 2023	0,34	2,87	-4,46	-7,78
Acumulado em doze meses	3,54	3,16	-6,86	-11,21

Fonte: Ipea, Instituto Brasileiro de Geografia e Estatística (IBGE) e FGV.

Elaboração: Grupo de Conjuntura da Diretoria de Estudos e Políticas Macroeconômicas (Dimac) do Ipea.

Tabela 4 – ICTI versus índices amplos de preços de outras fontes (JUN2023).

ICTI: variação em doze meses, peso e impacto por grupos (jul./2022-jun./2023)

Grupo	Variação (%)	Peso	Impacto (p.p.)
Índice Geral	3,54	1	3,54
Pessoal	7,24	0,44	3,19
Serviços profissionais e outros	12,37	0,15	1,89
Aluguel de imóveis	6,59	0,02	0,13
Demais despesas operacionais	-6,85	0,18	-1,24
Comunicação	0,43	0,01	0,01
Energia elétrica	1,17	0,01	0,01
Depreciação e amortização	-2,37	0,05	-0,12
Material de consumo	-2,37	0,13	-0,32

Fonte: Ipea.

Elaboração: Grupo de Conjuntura da Dimac/Ipea.

Tabela 5 – ICTI: variação em 12 meses, peso e impacto por grupos (JUL2022 – JUL2023).

Na desagregação pelos oito grupos de serviços que compõem o ICTI (Tabela 5), observa-se que, no acumulado em doze meses, a maior contribuição veio do segmento de despesas com profissionais. O segmento referente as demais despesas operacionais também afetou o ICTI.

8.3. – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

8.3.1. - SOLUÇÃO A: LOCAÇÃO DOS ATIVOS DE TIC PARA A EXECUÇÃO DO SERVIÇO:

De maneira geral, a duração dos contratos regidos pelo Art. 105 da Lei nº 14.133/21 será a prevista em edital, e deverão ser observadas, no momento da contratação e a cada exercício financeiro, a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro. Todavia, existem relações contratuais que, pela sua natureza, levaram o legislador a prever hipóteses de



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

exceção a essa regra.

Essas exceções estão previstas nos Art. 106 e 107 da Lei nº 14.133/21, importando, para a situação em exame, no que diz respeito à duração dos contratos regidos por esta Lei:

Art. 106: “a Administração poderá celebrar contratos com prazo de até 5 (cinco) anos nas hipóteses de serviços e fornecimentos contínuos, observadas as seguintes diretrizes:

I – a autoridade competente do órgão ou entidade contratante deverá atestar a maior vantagem econômica vislumbrada em razão da contratação plurianual.

II – a Administração deverá atestar, no início da contratação e de cada exercício, a existência de créditos orçamentários vinculados à contratação e a vantagem em sua manutenção.

III – a Administração terá a opção de extinguir o contrato, sem ônus, quando não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

§ 1º A extinção mencionada no inciso III do caput deste artigo ocorrerá apenas na próxima data de aniversário do contrato e não poderá ocorrer em prazo inferior a 2 (dois) meses, contado da referida data.

§ 2º Aplica-se o disposto neste artigo ao aluguel de equipamentos e à utilização de programas de informática”.

Art. 107: “os contratos de serviços e fornecimentos contínuos poderão ser prorrogados sucessivamente, respeitada a vigência máxima decenal, desde que haja previsão em edital e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes”.

De acordo com os Art. 106 e 107, admite-se a prorrogação dos contratos de prestação de serviços continuados, respeitadas as suas disposições, envolvendo a previsão orçamentária e a existência de vantagens para a Administração.

Diante do contexto legal, foram observados elementos de natureza funcional e orçamentária que conflitam com a realidade do CIM. Um contrato de locação exige uma previsão orçamentária por um período de até 5 anos, porém esta previsão não tem ocorrido na Administração atual, inviabilizando a “Solução A”.

Outro motivo que inviabiliza a presente solução é devido às características dos dados manipulados e das informações classificadas, que necessitam da implantação de cuidados, regras de segurança da informação e de segurança orgânica para os equipamentos sejam utilizados pelo CIM e, potencialmente, por outras Organizações Militares da MB relacionadas ao setor cibernético. No término do período de locação, estes softwares e equipamentos devem retornar ao seu proprietário e esta situação



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

poderia, em tese, causar o acesso a documentos classificados por pessoas ou instituições não autorizadas.

Cabe ressaltar que diz respeito a uma solução de gestão de risco cibernético, não há disponibilidade de locação dos ativos de TIC

Portanto, conclui-se que a “Solução A” é inviável de ser praticada no âmbito do CIM, não dispondo de viabilidade para cálculo do TCO.

8.3.2. - SOLUÇÃO B: AQUISIÇÃO DA ESTRUTURA DE TIC PARA A HOSPEDAGEM DA SOLUÇÃO DE GESTÃO DE RISCO CIBERNÉTICO:

O mercado de Tecnologia da Informação e Comunicações (TIC) é marcado pela evolução contínua, pela mudança de padrões e, conseqüentemente, pela incerteza do futuro. Nesse cenário, os gestores de TIC são constantemente chamados a tomar decisões estratégicas em curto prazo, baseados nas suas experiências e discernimento pessoais, em informações esparsas oriundas da Internet, ou informações advindas dos fornecedores que comprometem a imparcialidade das análises.

Nesse sentido, a diversidade de informações, muitas vezes contraditórias ou infundadas sobre tecnologia, torna necessária a identificação de fontes confiáveis para a obtenção e seleção dessas informações, bem como de ferramentas e técnicas que permitam sua efetiva utilização e que habilitem os gestores de TIC a transformá-las em conhecimento para a tomada de decisões.

Em relação aos ativos de TIC que se pretende contratar, faz-se necessário uma visão imparcial para subsidiar os trabalhos de prospecção e definição de soluções nos diversos segmentos tecnológicos, objeto do “Plano Diretor de Tecnologia da Informação e Comunicação” (PDTIC) do CIM.

A solução de aquisição da estrutura de TIC para hospedar uma solução de gestão de risco cibernético se baseia nesta análise, onde os gestores e técnicos em TIC poderiam encurtar o processo de escolha e decisão de adoção das tecnologias, as quais atendem as demandas para que são destinadas, onde devem ser empregadas, quais benefícios apresentam e em quais situações devem ser utilizadas. Além disso, com a obtenção definitiva, pode-se fazer o monitoramento do ciclo de amadurecimento das tecnologias, indicando quando elas estarão no seu estágio de menor ou maior risco, podendo assim evitar tecnologias com grande grau de imaturidade ou obsolescência, minimizando os riscos e os desafios que comumente são traduzidos em atrasos, inoperâncias, riscos da área da Segurança da Informação e aumento de custo na manutenção.

A análise e comparação entre os custos totais de propriedade (TCO) das soluções identificadas utilizou como premissa de referência não se tratar de uma migração de recursos de TIC para a nuvem .

Para a análise do TCO utilizou-se com referência os custos de se prover elasticidade,



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

autoprovisionamento de recursos e alocação de grupos (*pools*) de recursos sob demanda para determinado projeto. Dessa forma, a tabela a seguir apresenta a comparação do custo marginal de aprovisionamento de recursos para o projeto com essa característica de necessidades de negócio.

Para um cenário de acréscimo computacional, considerou-se uma demanda com necessidade de 10 máquinas virtuais com 4 CPUs, 8 GB de RAM, 500 TB de armazenamento em SAN, um ativo de rede, por um período de 3 anos, tem-se a seguinte comparação:

- Hospedagem local de toda a infraestrutura: tendo como base que a instituição já possui um *Data Center*, o cálculo da hospedagem local considerará apenas a estrutura estritamente necessária para a solução:
 - Servidor de Aplicação tipo *rack*;
 - Armazenamento (*storage*);
 - Ativo de rede – comutador (*switch*);
 - Cálculo do Custo do Planejamento da Licitação; e
 - Aquisição de uma solução de gestão de risco cibernético (*software*).

CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE PARA A SOLUÇÃO B:

Servidor de aplicação do tipo <i>rack</i> :						
	Qtd.	Valor de Ref.	12 meses	12 meses	12 meses	Total por Item
Custo do servidor	2	R\$ 65.000,00	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 130.000,00
Custo energético	2	R\$ 165,60	R\$ 3.974,40	R\$ 3.974,40	R\$ 3.974,40	R\$ 11.923,20
Custo da manutenção	2	R\$ 30,00	R\$ 720,00	R\$ 720,00	R\$ 720,00	R\$ 2.160,00
Total do Item						R\$ 144.083,20
Cálculo do Custo de Energia por Unidade						
Potência da Fonte da CPU	Kw	Hr Func.	Dias Func.	Total Kw/h	Valor Kw/h	Custo mensal
Potência da Fonte do Monitor	0,4	24	30	288	R\$ 0,58	R\$ 165,60
	0	8	20	0	R\$ 0,58	R\$ 0,00
						R\$ 165,60

* Valores obtidos na Tabela SINAPI – DF – JUN2023



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

Armazenamento (storage):

	Qtd.	Valor de Ref.	12 meses	12 meses	12 meses	Total por Item
Custo do armazenamento	2	R\$ 233.311,85	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 466.623,70
Custo energético	2	R\$ 289,80	R\$ 6.955,20	R\$ 6.955,20	R\$ 6.955,20	R\$ 20.865,60
Custo da manutenção	2	R\$ 30,00	R\$ 720,00	R\$ 720,00	R\$ 60,00	R\$ 1.500,00
Total do item						R\$ 488.989,30

Cálculo do Custo de Energia por Unidade

	Kw	Hr Func.	Dias Func.	Total Kw/h	Valor Kw/h	Custo mensal
Potência da Fonte da CPU	0,4	24	30	288	R\$ 0,58	R\$ 165,60
Potência da Fonte do Monitor	0,3	24	30	216	R\$ 0,58	R\$ 124,20
						R\$ 289,80

* Valores obtidos na Tabela SINAPI – DF – JUN/2023

Ativo de rede: comutador (switch):

	Qtd.	Valor de Ref.	12 meses	12 meses	12 meses	Total por Item
Custo da solução	1	R\$ 6.084,33	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 6.084,33
Custo energético	1	R\$ 9,20	R\$ 110,40	R\$ 110,40	R\$ 110,40	R\$ 331,20
Custo da manutenção	1	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 0,00	R\$ 0,00
Total do item						R\$ 6.415,53

Cálculo do Custo de Energia por Unidade

	Kw	Hr Func.	Dias Func.	Total Kw/h	Valor Kw/h	Custo mensal
Potência da Fonte	0,1	8	20	16	R\$ 0,58	R\$ 9,20

* Valores obtidos na Tabela SINAPI – DF – JUN2023

Cálculo do Custo do Planejamento da Licitação:

H/H Nível superior	R\$ 79,61	R\$ 12.737,60
H/H Nível Médio	R\$ 30,00	R\$ 4.800,00
Horas Trabalhadas	160	
Militares/Servidores Nível Superior		3
Militares Nível Médio		3
Total do item:		R\$ 52.612,80



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

Consolidação dos valores:	
Servidor de aplicação tipo rack	R\$ 144.083,20
Armazenamento (storage)	R\$ 488.989,30
Ativo de rede: comutador (switch)	R\$ 6.415,53
Cálculo do Custo do Planejamento da Licitação	R\$ 52.612,80
Total	R\$ 692.100,83

O custo inicial e aproximado para esta solução é de R\$ 692.100,83 (seiscentos e noventa e dois mil, cem reais e oitenta e três centavos). Considerando o custo da “Solução B”, ele já ultrapassa em mais de quatro vezes o custo da “Solução C” (será detalhada a seguir), além de ainda ser necessário comprar uma solução de gestão de risco cibernético (software), de maneira proprietária, para hospedar na infraestrutura em tela, tornando-se inviável pelo custo e pela não disponibilidade no mercado de aquisição do software nesta modalidade.

8.3.3. - SOLUÇÃO C: CONTRATAÇÃO NA MODALIDADE “SOFTWARE COMO SERVIÇO” (SAAS – “SOFTWARE-AS-A-SERVICE”):

A disponibilização de programas, aplicações e ferramentas pela Internet, sem a necessidade de instalação ou atualização de software localmente, tem se consolidado no mercado de TIC. Neste caso, todos os dados gerados devem ser armazenados em ambiente próprio, no fornecedor, uma vez que só é disponibilizado ao cliente a utilização do software no formato de uma plataforma *online* de serviços.

O custo total de propriedade (TCO) de SaaS para aplicações em nuvem geralmente são mais baixos que soluções com hospedagem local. Isso ocorre devido à eliminação dos custos de hardware, manutenção, atualizações e necessidade de ativos físicos.

8.3.3.1. - Análise Técnica desta solução existente no mercado

As soluções de avaliação de risco cibernético identificadas no mercado, com boa avaliação e comentários favoráveis no portal da *Gartner*, foram listadas conforme o disposto nos itens 6.1.3 e 6.2.

A aquisição de uma plataforma de gestão de risco cibernético, na modalidade SaaS, de acordo com os requisitos levantados neste ETP, será realizada por meio de Pregão Eletrônico por menor preço global.

A equipe de planejamento da contratação verificou que a aquisição de 01 (uma) licença de uso da plataforma *Security Scorecard Ratings*, ou da *BitSight Security Ratings Platform*, ou da *RiskRecon Ratings*, pelo período de 12 (doze) meses, é satisfatória, uma vez que é técnica e economicamente viável e atende a todas as necessidades elencadas.



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

A aquisição da licença mencionada não gerará despesas adicionais com capacitação dos profissionais, uma vez que, esse software já é amplamente utilizado nas comunidades de Inteligência e possui uma ampla bibliografia.

A aquisição da licença trará resultados imediatos para o Centro, uma vez que, o software já possui sua plataforma estável, não sendo necessário nenhum tempo adicional para a implantação, desenvolvimento ou customização da ferramenta.

O custo aproximado para esta solução é de R\$ 180.000,00 (cento e oitenta mil reais)

8.3.3.2. - Aquisição de licenças de outro software similar

Embora tenha sido solicitado a aquisição de um software específico, existe a possibilidade de aquisição de licenças de softwares similares, que possuam as mesmas características, e que devam atender a todas as necessidades e requisitos levantados.

8.3.4. - SOLUÇÃO D: DESENVOLVIMENTO DE UM SISTEMA SIMILAR, PELA PRÓPRIA MB, QUE ATENDAS AS NECESSIDADES ELECADAS NESTE ETP

Esta solução foi considerada inviável, devido à falta de orçamento, disponibilidade de pessoal técnico dedicado e conhecimento técnico na MB suficientes para conceber e manter uma solução de gestão de risco cibernético de maneira longa e adequada ao propósito de sua utilização. Não foi possível realizar o calculo de TCO.

8.4. - MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos			Viabilidade	Total
	Ano 1	Ano 2	Ano 3		
Solução A	XXX	XXX	XXX	NÃO	XXX
Solução B	XXX	XXX	XXX	NÃO	XXX
Solução C	R\$180.000,00	R\$180.000,00	R\$180.000,00	SIM	R\$540.000,00
Solução D	XXX	XXX	XXX	NÃO	XXX



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

9. - DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Solução C: plataforma de gestão de risco cibernético, na modalidade SaaS, por meio de uma assinatura anual (12 meses) do serviço, para acesso em tempo real às informações de risco cibernético, incluindo métricas e indicadores de risco, *benchmarking* setorial, contemplando a sugestão de medidas de correção atualizadas à organização de interesse, além de funcionalidades relacionadas ao monitoramento de fornecedores, terceiros e parceiros estratégicos.

10. - ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Sob a perspectiva de estimativa, para a contratação de uma plataforma compatível com os requisitos levantados neste ETP, adequada no que concerne a “Solução C”, o custo Total da Contratação será de R\$180.000,00 (cento e oitenta mil reais).

11. - DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

O presente Estudo Técnico Preliminar, elaborado pelos integrantes Técnico e Requisitante em harmonia com o disposto no art. 11 da Instrução Normativa nº 01/2019/SGD, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE DA CONTRATAÇÃO, uma vez considerados os seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade.

Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que RECOMENDAMOS o prosseguimento da pretensão contratual.

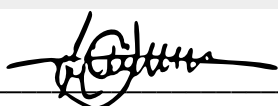


**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

12. - ASSINATURAS

A Equipe de Planejamento da Contratação foi instituída pela Ordem de Serviço nº XXX, de de outubro de 2023.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
 CF Flávio de Queiroz Guimarães NIP: 87.3012.11 Brasília, 24 de novembro de 2023.	 CT(T) Mauricio Fuginiti Olivaes Munhoz NIP: 09.0022.01 Brasília, 24 de novembro de 2023.



**MINISTÉRIO DA DEFESA
MARINHA DO BRASIL
CENTRO DE INTELIGÊNCIA DA MARINHA**

13. - APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

**AUTORIDADE MÁXIMA DA ÁREA DE TIC
(OU AUTORIDADE SUPERIOR, SE APLICÁVEL - § 3º do art. 11)**

Assinatura manuscrita em tinta preta, sobre uma linha horizontal.

CMG(RM1-T) José Henrique Wanderley Ribeiro
IIP/81.9029.81

Brasília, 24 de novembro de 2023.