

TERMO DE REFERÊNCIA nº 01/2023

Processo Administrativo nº 61272.001791/2023-84

Referência: Artigos 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022.

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

- 1.1. Este Termo de Referência (TR) tem por objetivo apresentar os requisitos técnicos, as condições comerciais e os prazos para a seleção de uma plataforma de gestão de risco cibernético, que fará parte das atividades desempenhadas pelo Centro de Inteligência da Marinha (CIM), Organização Militar da Marinha do Brasil (MB). A contratação será feita nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATSER	MÉTRICA	CÓD. PMC-TIC	QTD.	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Gestão de Risco Cibernético	26077	Disponibilização do serviço 24 horas por dia, 7 dias por semana, durante 12 meses.	N/A	Subscrição	180.000,00	180.000,00

- 1.2. O serviço objeto desta contratação é caracterizado como comum, uma vez que as empresas prestadoras existentes no mercado para o serviço em tela operam sob Contratos convencionais com seus clientes das esferas pública e privada.
- 1.3. O serviço pretendido baseia-se na escolha da proposta mais vantajosa para a contratação da solução de gestão de risco cibernético, conforme condições expressas neste TR.
- 1.4. O critério de julgamento para escolha do fornecedor da solução adotado será o menor preço, observadas as exigências contidas neste TR quanto às especificações do objeto.
- 1.5. A empresa vencedora firmará um Contrato por tempo determinado, por 12 (dode) meses, e passível de renovação com a MB para o fornecimento da plataforma de gestão de risco cibernético que atenda às especificações descritas neste TR, na forma do Art. 105 da Lei nº 14.133, de 2021.
- 1.6. A minuta do Contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

- 2.1. A descrição da solução como um todo se encontra pormenorizada em tópico específico dos Estudos Técnicos Preliminares, anexo deste TR.
- 2.2. A solução de gestão do risco cibernético abrangerá as organizações e instituições que mantenham contratos, parcerias estratégicas ou vínculos com a MB, incluindo a própria Força, a fim de que sejam identificados e categorizados os riscos cibernéticos institucionais.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

- 3.1. A presente contratação justifica-se na relação com a atividade fim do Centro de Inteligência da Marinha (CIM) em produzir 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) de interesse no nível tático.
- 3.2. 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.

- 3.3. O CIM, a fim de assessorar o processo decisório do Comandante da Marinha 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.
- 3.4. A contratação de uma solução de gestão de risco cibernético propiciará ao CIM: o incremento da consciência situacional do ECiber nacional, ECiber-MB e ECiber de interesse, aumento da eficácia na coleta de dados de Contrainteligência Cibernética, o mapeamento de vulnerabilidades da MB e de parceiros estratégicos, a potencial constatação da existência ameaças cibernéticas institucionais, a identificação e categorização de diversos aspectos a compor o risco cibernético de uma organização, a identificação das atividades maliciosas na Deep Web e Dark Web que envolvam as instituições prestadoras de serviço e parceiros envolvidos nos projetos estratégicos da Força, com potencial de impacto no ECiber da MB.
- 3.5. Uma solução de gestão de risco cibernético atenderá às expectativas e exigências da MB e do CIM, mantendo o grau de confiabilidade, segurança, disponibilidade, integridade e desempenho para a condução de suas atividades institucionais. Desta forma, e a fim de atender às demandas técnicas do setor cibernético, torna-se necessária a aquisição de uma solução para apoiar as demandas de Contrainteligência Cibernética.
- 3.6. O objeto deste Termo de Referência abrangerá 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.
- 3.7. O modelo conceitual que melhor ilustra a solução a ser obtida seria de um sistema de gestão de risco cibernético integrado, apresentando os dados de forma textual e gráfica, no que couber, permitindo a extração de relatórios das análises.
- 3.8. Pretende-se, ainda, que a solução seja acompanhada dos seguintes serviços: o 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; e o Suporte Técnico, provido em português do Brasil, na modalidade à distância.
- 3.9. O objeto da contratação também está alinhado com o arcabouço normativo atinente ao setor cibernético no âmbito das Forças Armadas, da MB e do CIM:

ALINHAMENTO AO PLANEJAMENTO ESTRATÉGICO DA MARINHA		
ID	Objetivos Estratégicos	Nome do documento e vigência
1	Objetivo Naval 8 (OBNAV8) “Desenvolver a capacidade cibernética da MB”	Plano Estratégico da Marinha 2040 (PEM2040)
2	Objetivo Naval 9 (OBNAV9) “Aprimorar as Inteligências estratégica e operacional”	Plano Estratégico da Marinha 2040 (PEM2040)

ALINHAMENTO AO PDTIC 2020-2023			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
OE-TI 6	Objetivo Estratégico 6: Fortalecer a capacidade da Marinha de atuar na defesa do ambiente cibernético.	M7	Implementar, aprimorar e manter soluções tecnológicas informacionais
		M8	Implementar e aprimorar processos de tratamento de dados
		M9	Fomentar as ações de Segurança da Informação e Comunicações

ALINHAMENTO ÀS POLÍTICAS, DOCTRINAS E NORMAS 2023	
Item	Descrição
1	Constituição da República Federativa do Brasil: “Art. 142. As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem”.
2	Política Nacional de Defesa (PND): Decreto 5.484, de 30 de junho de 2005 - “A Política Nacional de Defesa estabelece como fundamento no ambiente nacional que “2.2.16 Adicionalmente, requerem especial atenção a segurança e a defesa do espaço cibernético brasileiro, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional”.
3	Estratégia Nacional de Defesa (END): Decreto nº 6.703, de 18 de dezembro de 2008 - “A Estratégia Nacional de Defesa estabelece os setores estratégicos para o país, entre eles os três setores tecnológicos essenciais para a Defesa Nacional: o nuclear, o cibernético e o espacial, devendo ser fortalecidos. Define, ainda, como Ações Estratégicas de Defesa e de fortalecimento da capacidade de dissuasão: “Desenvolver as capacidades de monitorar e controlar o espaço aéreo, o espaço cibernético, o território, as águas jurisdicionais brasileiras e outras áreas de interesse (AED – 10)” e “Incrementar as capacidades de defender e de explorar o espaço cibernético (AED – 11)”.
4	Doutrina Militar de Defesa Cibernética: Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014 - “Em seu Capítulo II – Fundamentos, a Doutrina Militar de Defesa Cibernética diz: “2.1.1 A partir do estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa, em 2008, dois campos distintos passaram a ser reconhecidos: a Segurança Cibernética, a cargo da Presidência da República (PR), e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas”. “O Capítulo III – Sistema Militar de Defesa Cibernética (SMDC) traz a definição: “3.1.1 A Defesa Cibernética, por ser um dos componentes da Defesa Nacional, é missão das Forças Armadas (FA), conforme a legislação referenciada no capítulo I. Entretanto, as peculiaridades do Espaço Cibernético tornam impraticável o cumprimento dessa missão se não houver o comprometimento da sociedade como um todo, imbuída do sentimento de responsabilidade individual e coletiva pela proteção das infraestruturas críticas nacionais no Espaço Cibernético”.
5	Política Cibernética de Defesa (PCD): Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012 - “A Política Cibernética de Defesa tem como um de seus objetivos: “colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR)”.
6	Política Nacional de Inteligência (PNI): Decreto 8.793, de 29 de junho de 2016 - “A Política Nacional de Inteligência considera como principais ameaças àquelas que apresentem potencial capacidade de pôr em perigo a integridade da sociedade e do Estado e a Segurança Nacional do Brasil. Sobre o tema, a PNI traz: “O desenvolvimento das tecnologias da informação e das comunicações impõe a atualização permanente de meios e métodos, obrigando os órgãos de Inteligência - no que se refere à segurança dos siste-

ALINHAMENTO ÀS POLÍTICAS, DOCTRINAS E NORMAS 2023	
Item	Descrição
	mas de processamento, armazenamento e proteção de dados sensíveis - a resguardar o patrimônio nacional de ataques cibernéticos e de outras ações adversas, cada vez mais centradas na área econômico-tecnológica. A crescente interdependência dos processos produtivos e dos sistemas de controle da tecnologia da informação e comunicações desperta preocupação quanto à segurança do Estado e da sociedade, em decorrência da vulnerabilidade a ataques eletrônicos, ensejando atenção permanente da Inteligência em sua proteção”. “Em seu item 8.4 - Expandir a capacidade operacional da inteligência no espaço cibernético, a PNI descreve a necessidade de ações preventivas da inteligência cibernética como: “Por sua vez, a rede mundial de computadores, além de canal cada vez mais propício à perpetração de atos protagonizados por agentes do crime organizado ou por organizações terroristas, tem-se constituído, ainda, em espaço privilegiado de discussões, diversas das quais relativas aos interesses do País. Nesse contexto, é primordial acompanhar, avaliar tendências, prevenir e evitar ações prejudiciais à consecução dos objetivos nacionais”.
7	Estratégia Nacional de Inteligência (ENI): Decreto nº 14.503, de 15 de dezembro de 2017 - “A Estratégia Nacional de Inteligência identifica como desafios a ampliação e o aperfeiçoamento do processo de capacitação para atuação na área de Inteligência, maior utilização de tecnologia de ponta, especialmente no campo cibernético, intensificação do uso de tecnologias de tratamento, análise de grandes volumes de dados (Big data e Analytics) e apoio ao combate à corrupção, ao crime organizado, aos ilícitos transnacionais e ao terrorismo”.

- 3.10. O presente Termo de Referência não se trata de serviços públicos digitais, não cabendo a integração do objeto da contratação à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste documento.
- 3.11. 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.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio:

4.2. A presente contratação orienta-se pelos seguintes requisitos de negócio:

- 4.2.1. Incremento na consciência situacional sobre o ECiber nacional, ECiber-MB e ECiber de interesse;
- 4.2.2. Aumento da eficácia na coleta de dados de Contraineligência Cibernética;
- 4.2.3. Mapeamento de vulnerabilidades da MB, de parceiros estratégicos e de organizações de interesse;
- 4.2.4. Potencial constatação da existência ameaças cibernéticas institucionais;
- 4.2.5. 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;
- 4.2.6. Acompanhamento baseado na Inteligência de Ameaças Cibernéticas no ECiber nacional, ECiber-MB e ECiber de interesse; e

4.2.7. Identificação e categorização de diversos aspectos a compor o risco cibernético de uma organização de interesse.

4.3. Requisitos de Capacitação:

4.4. É necessária uma instrução inicial sobre a utilização da solução para os usuários designados. A capacitação deverá ser de no mínimo 04 (quatro) horas de duração, podendo ser ofertada em diferentes modalidades.

4.5. A capacitação poderá ocorrer por meio de treinamento presencial, e/ou a disponibilização de um *workshop* à distância, e/ou oferta de um tutorial de utilização com manual por escrito e apresentações gravadas em vídeos, suficientes ao bom uso das capacidades da solução.

4.6. Requisitos Legais:

4.7. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei nº 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis;

4.8. Requisitos Técnicos:

4.9. 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:

4.9.1. Exposição às vulnerabilidades não corrigidas (CVE, zero-day, ativos de rede com versões obsoletas, soluções de TIC com versões obsoletas);

4.9.2. Histórico da ocorrência de incidentes cibernéticos nos últimos 12 meses;

4.9.3. Histórico do vazamento de dados sigilosos e credenciais de acesso – ex.: e-mails corporativos, sistemas internos e serviços on-line;

4.9.4. 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;

4.9.5. Avaliação do estado e exposição do DNS no domínio principal e subdomínios;

4.9.6. Indicador do nível de segurança da rede de dados da organização, em caráter de projeção ou preditivo;

4.9.7. Exposição da organização alvo às técnicas de engenharia social e de dados que sejam entendidos como uma vulnerabilidade de segurança organizacional;

4.9.8. 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;

4.9.9. Quando os dados coletados permitirem, apresentar um indicador do nível de governança em TIC;

4.9.10. Exibir dados sobre a segurança das aplicações, informações e serviços disponibilizados por meio dos sites da organização;

4.9.11. Exposição na Deep Web e Dark Web: presença de dados sensíveis da organização em fóruns hacker;

4.9.12. Exibir dados sobre infecções por malwares atrelados às botnets;

4.9.13. Exibir dados sobre propagação de spam;

- 4.9.14.** Existência de dados em servidores de malware (ransomware, wiper, trojan, RAT) que possam levar à inferência de infecção da organização de interesse;
- 4.9.15.** Existência de comunicações não solicitadas externamente, como por exemplo, port-scan originários da infraestrutura da própria organização de interesse;
- 4.9.16.** Exibir dados sobre sistemas executando aplicativos potencialmente indesejados, como por exemplo: adware; e
- 4.9.17.** Exibir a infecção de malwares específicos por nome, além de fornecer detalhes e instruções de correção.
- 4.10.** As coletas de dados não intrusivas do espaço cibernético da organização de interesse, preferencialmente, cobrirão os seguintes aspectos tecnológicos em caráter de detalhamento:
 - 4.10.1.** Endereços IP da borda da rede (visibilidade para a Internet):
 - 4.10.1.1. Portas de serviço ou aplicação abertas sem necessidade;
 - 4.10.1.2. Serviço de proxy anônimo;
 - 4.10.1.3. Existência de indicadores de ataque, ou do inglês Indicator of Attack (IoA);
 - 4.10.1.4. Existência de indicadores de comprometimento, ou do inglês Indicator of Compromise (IoC);
 - 4.10.1.5. Vulnerabilidades em certificados SSL/TLS (certificados expirados, autoassinados, revogados, com vida útil com tempo muito longo, emprego de algoritmo inadequado);
 - 4.10.1.6. Presença de malwares (ransomwares, wipers, bots, Remote Access Trojans - RAT) enviando sinal de beacon ao servidor de comando e controle (C2) de ator adverso;
 - 4.10.1.7. Presença de nós da rede TOR;
 - 4.10.1.8. Presença de servidores de compartilhamento de arquivos peer-to-peer associados aos torrents; e
 - 4.10.1.9. Presença de servidores de C2 dentro da rede de dados da organização.
 - 4.10.2.** Vazamento de dados:
 - 4.10.2.1. Exposição de credenciais de acesso de e-mails corporativos e sistemas institucionais;
 - 4.10.2.2. Histórico de credenciais de acesso vazadas nos últimos 12 meses;
 - 4.10.2.3. Temas relacionados ao Domain Name Server (DNS);
 - 4.10.2.4. Existência de acesso irrestrito às configurações dos registros DNS;
 - 4.10.2.5. Existência de registros inválidos nos DNS utilizados pela organização;
 - 4.10.2.6. Presença do serviço de OpenDNS competindo com os redirecionamentos dos DNS organizacionais; e
 - 4.10.2.7. Existência de falhas ou vulnerabilidades relacionados à implementação de DNSSEC.
 - 4.10.3.** Segurança da rede de dados da organização:
 - 4.10.3.1. Detecção da presença do serviço de Elasticsearch de forma ostensiva na rede de dados;
 - 4.10.3.2. Exposição de serviço FTP exposto à Internet;
 - 4.10.3.3. Exposição de serviços IMAP/POP3 à Internet de maneira insegura;

- 4.10.3.4. Detecção de redes industriais/operacionais que hospedam sistemas ICS/SCADA expostos à Internet;
- 4.10.3.5. Detecção de impressoras, câmeras IP e de ativos de segurança organizacional presentes na rede de dados da organização expostos à Internet;
- 4.10.3.6. Exposição de serviços como Samba (protocolo SMB), LDAP ou Active Directory à Internet; e
- 4.10.3.7. Exposição do serviço e/ou das respectivas interfaces de acesso aos bancos de dados da organização (Microsoft SQL Server, Oracle Database, MySQL, PostgreSQL, MongoDB e similares).
- 4.10.4. Questões relacionadas às ofensivas de hackers:**
 - 4.10.4.1. Domínio(s), subdomínio(s) e endereço(s) IP públicos da organização sendo relacionados em investidas hacker nos últimos 12 meses; e
 - 4.10.4.2. Domínio(s) e subdomínio(s) sendo relacionados como vítimas em casos de ransomware, wiper, bot ou RAT nos últimos 12 meses.
- 4.10.5. Patches de correção e versão corrente dos ativos informacionais:**
 - 4.10.5.1. Ativos informacionais no fim da vida útil ou considerados obsoletos;
 - 4.10.5.2. Observação de vulnerabilidades relacionadas aos Common Vulnerabilities and Exposures (CVE) de alta, média e baixa criticidade; e
 - 4.10.5.3. Observação de vulnerabilidades do tipo zero-day conhecidas nas versões dos ativos informacionais em uso.
- 4.10.6. Engenharia social:**
 - 4.10.6.1. Exposição de dados de pessoal em caráter corrente;
 - 4.10.6.2. Existência de vazamentos de dados sensíveis da organização em bancos de dados nos fóruns hacker; e
 - 4.10.6.3. Histórico de exposição de dados de pessoal nos últimos 12 meses.
- 4.10.7. Segurança das aplicações (web):**
 - 4.10.7.1. Gestão inadequada de configuração dos servidores de hospedagem web;
 - 4.10.7.2. Padrão de redirecionamento em protocolos HTTP/HTTPS realizados de forma insegura;
 - 4.10.7.3. Configurações incorretas ou vulneráveis na utilização dos protocolos SSL e TLS; e
 - 4.10.7.4. Gerenciadores de conteúdo configurados de maneira não segura e/ou com vulnerabilidades conhecidas.
- 4.11. Fornecer uma visão geral das organizações monitoradas, com indicadores de risco cibernético e seus vetores avaliados no ECiber.**
- 4.12. 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.**
- 4.13. 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 e de porte equivalente, etc.).**

- 4.14.** 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.
- 4.15.** 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).
- 4.16.** A solução deve fornecer recursos analíticos profundos, incluindo a capacidade de entender o desempenho relativo da organização no contexto de pares (organizações de natureza e 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.
- 4.17.** A funcionalidade de gestão do risco cibernético propriamente dito deve ter, no mínimo, as seguintes características:
- 4.17.1.** Atualizações diárias, para cada entidade monitorada;
- 4.17.2.** Dados de histórico diário até os 12 meses anteriores, desde que a empresa esteja monitorada na solução;
- 4.17.3.** O scan automático das vulnerabilidades da organização de interesse deve ocorrer até o máximo de 30 dias;
- 4.17.4.** Cada vetor de risco que compõem a classificação deve ser avaliado individualmente, com uma métrica própria para atribuição do nível de risco;
- 4.17.5.** Preferencialmente, a correlação entre vazamentos de dados e a avaliação do risco cibernético poderá ser validada independentemente por meio de um terceiro;
- 4.17.6.** 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;
- 4.17.7.** 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;
- 4.17.8.** Scan de todos os IP 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;
- 4.17.9.** 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;
- 4.17.10.** 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, para português do Brasil. Caso não seja possível, os relatórios deverão ser disponibilizados em Inglês;

- 4.17.11. 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;
- 4.17.12. 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;
- 4.17.13. A metodologia tem de ser pública e disponibilizada na internet, bem como os dados devem fornecidos a qualquer usuário ou empresa que os solicite; e
- 4.17.14. 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.
- 4.18. A solução deve ser capaz de mostrar rapidamente quais fornecedores apresentam incidentes significativos em seu ECiber.
- 4.19. A solução deve ser capaz de mostrar rapidamente quais fornecedores têm vulnerabilidades, e quais são elas.
- 4.20. A solução deve oferecer às organizações-alvo a capacidade de ver sua avaliação de risco cibernético gratuitamente.
- 4.21. A desenvolvedora da solução deverá ser considerada líder por, pelo menos, uma empresa de análise independente como a Forrester ou a Gartner.
- 4.22. 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.
- 4.23. Oferecer a possibilidade de customizar 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.
- 4.24. A “digital footprint” de todas as organizações mapeadas na solução têm de ser atualizadas automaticamente no mínimo a cada 30 dias, para validação “digital footprint”.
- 4.25. A solução deverá ter um mínimo de 10.000.000 de empresas, entidades e organizações já mapeadas na plataforma e disponível para monitoração imediata pelo usuário.
- 4.26. A solução para mapeamento de uma nova empresa, organização ou entidade, que 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.
- 4.27. 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.
- 4.28. A MB observará os dados forenses detalhados dos eventos detectados de qualquer organização que necessite monitorar.
- 4.29. 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.

- 4.30.** 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.
- 4.31.** 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.
- 4.32.** 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:
- 4.32.1.** Relatório resumido, contendo a avaliação do risco cibernético da organização de interesse e os vetores que compõe essa avaliação;
 - 4.32.2.** Relatório dos eventos e/ou vulnerabilidades encontrados das organizações monitoradas;
 - 4.32.3.** 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;
 - 4.32.4.** Relatórios de nível de problemas e eventos potencialmente prejudiciais ao ECiber de interesse;
 - 4.32.5.** Relatórios de comparação do risco cibernético e seus vetores entre as organizações monitoradas; e
 - 4.32.6.** Relatórios customizados de forma ad-hoc, com a possibilidade de o usuário selecionar os dados da organização de interesse conforme for conveniente.
- 4.33.** 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.
- 4.34.** A plataforma deverá incluir análise de ameaças cibernéticas, preferencialmente indicando a criticidade, quando houver suspeita de infecção, além de instruções de remoção da ameaça.
- 4.35.** 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.
- 4.36.** O tempo de resposta do Suporte Técnico deverá ser de, no máximo, 24 horas úteis.
- 4.37.** A solução deverá 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.
- 4.38.** 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;

4.39. 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 alvo dos atores de ameaça.

4.40. A solução deverá basear-se os indicadores em frameworks de segurança consolidados internacionalmente pela comunidade de TIC.

4.41. Requisitos de Manutenção:

4.42. Devido às características da solução pretendida, há necessidade de realização de manutenções corretivas, preventivas, adaptativas e evolutivas pela Contratada, visando à disponibilidade da solução, à precisão e à atualização dos dados apresentados, além do aperfeiçoamento de suas funcionalidades de coleta, dado o dinamismo do domínio cibernético.

4.43. Em caso de comportamento anômalo da plataforma, tais como falhas no acesso, no leiaute das telas, nos painéis de dados e nos relatórios, ou ainda outras dificuldades de ordem técnica que impactem a disponibilidade, a usabilidade ou a integridade dos dados apresentados, a Contratada deverá atuar, pelo menos em caráter preliminarmente, em até 24 horas úteis.

4.44. Requisitos Temporais:

4.45. Os serviços devem ser iniciados no prazo máximo de 30 (trinta) dias corridos, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pela Contratada e autorizado pela Contratante.

4.46. Na contagem dos prazos estabelecidos neste TR, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.47. 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.

4.48. Na execução dos serviços, deverão ser observados os seguintes prazos:

Atividade, Tarefa ou Serviço	Prazo máximo de início de atendimento	Prazo máximo de solução de problema
Início da prestação do serviço.	30 dias	30 dias
Disponibilidade da plataforma para utilização normal (sem prejuízo de suas funcionalidades) após o início do serviço.	Imediato/Contínuo	02 dias
Treinamento ou instrução inicial de utilização da plataforma.	05 dias após a assinatura do Contrato	15 dias após a assinatura do Contrato
Suporte técnico.	24 horas após a solicitação	07 dias após a solicitação inicial

4.49. Requisitos Sociais, Ambientais e Culturais:

4.50. A solução de gestão de risco cibernético, suas funcionalidades, relatórios, painéis, e mensagens, preferencialmente, serão oferecidos em português do Brasil. Caso não esteja disponível este requisito, a solução poderá ser disponibilizada em inglês.

4.51. Requisitos da Arquitetura Tecnológica:

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

- 4.53.** 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.
- 4.54.** A solução de gestão de risco cibernético pretendida deverá ser oferecida no formato “Software como Serviço”, ou do inglês “Software-as-a-Service” (SaaS).
- 4.55.** O serviço de Suporte Técnico deverá acompanhar nativamente a solução Contratada, por todo o período em que vigorar o Contrato do objeto deste TR.
- 4.56.** O treinamento do usuário acerca da utilização e administração da solução seguirá o descrito neste Termo.
- 4.57. Requisitos de Projeto e de Implementação:**
- 4.58.** A solução de gestão de risco cibernético será provida por meio de serviço hospedado em nuvem, na modalidade de “Software como Serviço”, ou do inglês “Software-as-a-Service” (SaaS), de responsabilidade da Contratada. Não serão necessários Requisitos de Projeto ou preocupações adicionais com a Implementação de qualquer software no ambiente computacional do CIM.
- 4.59. Requisitos de Implantação:**
- 4.60.** A solução de gestão de risco cibernético será provida por meio de serviço hospedado em nuvem, na modalidade de “Software como Serviço”, ou do inglês “Software-as-a-Service” (SaaS), de responsabilidade da Contratada. Não será necessário realizar a implantação de qualquer software no ambiente computacional do CIM.
- 4.61. Requisitos de Garantia e Manutenção:**
- 4.62.** Não se aplica, já que se trata de prestação de serviços.
- 4.63. Requisitos de Experiência Profissional:**
- 4.64.** Os serviços de Suporte Técnico deverão ser prestados por técnicos devidamente capacitados na solução em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.
- 4.65.** O Suporte Técnico será prestado na modalidade à distância, por meio de sistema de chamados técnicos da Contratada, e-mail ou telefone, desde que exista um técnico habilitado no produto e se comunique em português do Brasil.
- 4.66. Requisitos de Segurança da Informação e Privacidade:**
- 4.67.** A solução deverá prover ao administrador (ou outros usuários autorizados) a capacidade de ler todas as informações das trilhas de auditoria e deverá apresentar a trilha de auditoria de modo que seja compreensível para o usuário.
- 4.68.** A identificação do usuário na solução deverá seguir as seguintes recomendações:
- 4.68.1.** A solução deverá prover chave de identificação única para cada usuário;
- 4.68.2.** A solução deverá prover mecanismo seguro de recuperação de senha; e
- 4.68.3.** A solução deverá permitir o emprego de senha forte (são consideradas fortes senhas que possuem no mínimo 12 (doze) caracteres, contendo letras maiúsculas e minúsculas, números, pontuação e símbolos).
- 4.69.** A autenticação do usuário na solução deverá seguir as seguintes recomendações:
- 4.69.1.** A solução deverá requerer autenticação antes de qualquer ação;

- 4.69.2.** A solução deverá prover mecanismo seguro de tratamento de erros de Autenticação; e
- 4.69.3.** A solução não deve sempre exibir a mensagem de erro padrão de autenticação, como por exemplo, “usuário e/ou senhas incorretos”.
- 4.70.** A solução deverá prover canal seguro de comunicação para autenticação.
- 4.71.** A solução deverá impedir ataques do tipo: SQL Injection e OS Command Injection.
- 4.72.** A solução deverá impedir ataques do tipo: Buffer Overflow e Integer Overflow.
- 4.73.** A solução deverá implementar proteção contra-ataques de Cross-Site Request Forgery (CSRF).
- 4.74.** A solução deverá implementar proteção contra-ataques de Cross-Site Script (XSS).
- 4.75.** A solução deverá implementar proteção contra-ataques de Cross-Frame Script (XFS).
- 4.76.** A solução deverá implementar proteção contra-ataques de Path Transversal, Resource Injection e Path Manipulation.
- 4.77.** Deve ser informado o cabeçalho HTTP “Strict-Transport-Security” nas respostas do sistema ao navegador para que ele identifique que a aplicação só pode ser acessada via HTTPS.
- 4.78. Vistoria:**
- 4.79.** Não há necessidade de realização de avaliação prévia do local de execução dos serviços.
- 4.80. Outros Requisitos Aplicáveis:**
- 4.81.** A disponibilidade da solução deverá ser maior que 93,4% em 12 meses.
- 4.82.** As organizações selecionadas para serem acompanhadas pela solução deverão ser de caráter sigiloso, não sendo reveladas a terceiros.
- 4.83.** 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.
- 4.84.** A solução deverá ser compatível com os navegadores Google Chrome, Microsoft Edge e Mozilla Firefox nas suas versões mais atuais.
- 4.85.** A interface da solução deverá ser apresentada no(s) idioma(s) português do Brasil, preferencialmente, ou de forma alternativa em inglês.
- 4.86.** 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.
- 4.87.** 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.
- 4.88.** 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.
- 4.89.** 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 e na avaliação geral do risco cibernético.
- 4.90.** A MB poderá solicitar a alteração das credenciais de acesso dos usuários da plataforma conforme a sua necessidade.

- 4.91.** Preferencialmente, a plataforma contemplará uma tela inicial com informações consolidadas para visualização das organizações monitoradas e alertas cadastrados.
- 4.92.** 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.
- 4.93.** A plataforma deverá exibir todos os relatórios e gráficos em painéis de fácil leitura (dashboards).
- 4.94.** Preferencialmente, ter as informações apresentadas na plataforma disponíveis para o download em diferentes formatos, como: HTML, PDF ou CSV.
- 4.95. Sustentabilidade:**
- 4.96.** Não se aplicam critérios de sustentabilidade para a contratação de serviço proposto, tendo em vista tratar-se de contratação de “Software como Serviço” (SaaS). Por se tratar de um software sendo executado em uma solução em nuvem, não há critérios de sustentabilidade aplicáveis. Tais critérios seriam exigíveis para aquisições com hardware com software embarcado. Além disso, o uso de robôs para a coleta de dados e inteligência artificial resultam em economia e gestão mais eficaz de recursos relacionado ao serviço prestado.
- 4.97. Da exigência de carta de solidariedade:**
- 4.98.** Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do Contrato.
- 4.99. Subcontratação:**
- 4.100.** Não é admitida a subcontratação do objeto contratual.
- 4.101. Da apresentação de catálogos:**
- 4.102.** A licitante deverá apresentar os manuais, catálogos, folders, ou outros documentos técnicos, ou ainda, links públicos oficiais da solução exigida, para comprovação do atendimento às características técnicas especificadas neste TR.
- 4.103.** No conjunto de documentos apresentados pela licitante (folders/catálogos), para fins de aceitação pela Contratante, deverá vir indicando corretamente, o item, especificação, link ou documento, página e trecho que comprove o atendimento de cada item/subitem dos Requisitos Técnicos. Será aceito também a carta do fabricante com as comprovações, desde que não ultrapasse 50% dos itens técnicos deste TR.
- 4.104.** Deverá apresentar com clareza as informações aplicáveis e necessárias à perfeita caracterização da solução, de forma a permitir a correta identificação desta na documentação técnica apresentada.
- 4.105.** A Contratada deveria apresentar carta do fabricante da solução ofertada que demonstre que ela é empresa parceira e autorizada, apta a comercializar, licenciar, prestar serviços de Suporte Técnico e treinamento da solução ofertada, devendo obrigatoriamente constar o nome da licitante e seu CNPJ.
- 4.106.** Os documentos serão analisados, para fins de verificação do atendimento às características da solução especificada neste TR.
- 4.107.** A análise das características dos itens ofertados será procedida em cotejo com as especificações técnicas constantes deste instrumento, sendo admitidos itens com até 10% de especificações inferiores.

4.108. Os itens desprovidos dos documentos relacionados no item anterior serão passíveis de diligência, podendo, para tanto, a Contratante se valer de todos os meios possíveis, tais como consulta a site diversos, ligações a fabricantes ou exigência de documentos complementares, dentre outros.

4.109. Caso os documentos apresentados não sejam aprovados, por não atenderem às especificações previstas neste Edital, o licitante será desclassificado.

4.110. Na hipótese da proposta da licitante ser desclassificada, por não atendimento das especificações técnicas requeridas, serão convocadas as demais licitantes, obedecendo-se rigorosamente a ordem de classificação das propostas, seguindo-se aos mesmos moldes descritos nos itens anteriores.

4.111. A licitante vencedora que vier a ser contratada ficará obrigada ao cumprimento integral de sua proposta, ainda que algum item não tenham sido objeto de verificação na análise do manual/catálogo/folder.

4.112. Da verificação de amostra do objeto:

4.113. Será realizada verificação de amostra do objeto para averiguar se a solução apresentada pela licitante detém os requisitos mínimos necessários para realização do serviço a ser contratado, de acordo com as funcionalidades, procedimentos e critérios objetivos descritos neste TR.

4.114. A amostra do objeto poderá ser testada pelos representantes do CIM por até 5 (cinco) dias úteis, podendo ser considerada “conforme” ou “não conforme” diante dos requisitos estabelecidos por este TR.

4.115. Garantia da Contratação:

4.116. Não haverá exigência da garantia da contratação dos [artigos 96 e seguintes da Lei nº 14.133, de 2021](#), pelas razões constantes do Estudo Técnico Preliminar.

4.117. O Contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

4.118. Requisitos de habilitação:

4.119. A Contratada deverá comprovar possuir a qualificação técnica necessária para a execução dos serviços, mediante a apresentação dos seguintes documentos:

4.119.1. A Contratada deverá apresentar Atestado de Capacidade Técnica, emitido por pessoa jurídica de direito público ou privado, com comprovação de que o fornecedor já prestou o serviço a ser contratado objeto deste TR.

4.119.2. Poderá ser apresentado mais de um Atestado de Capacidade Técnica para a comprovação dos serviços a serem contratados.

4.119.3. A título de diligência, poderá ser requerida a apresentação dos Contratos que originaram os atestados, bem como quaisquer informações necessárias a esclarecer ou complementar a instrução do processo.

4.119.4. Apresentação de documentação falsa ensejará a aplicação das penalidades previstas em lei.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da Contratante:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do Contrato para acompanhar e fiscalizar a execução dos Contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no TR;

- 5.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 5.1.4. liquidar o empenho e efetuar o pagamento à Contratada, dentro dos prazos preestabelecidos em Contrato;
- 5.1.5. comunicar à Contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução;
- 5.1.6. definir a disponibilidade mínima de fornecimento da solução por parte do contratado, com base em pesquisas de mercado, quando aplicável;
- 5.1.7. requisitar a prestação dos serviços objeto desta contratação, na forma prevista neste TR e nas demais normas aplicáveis;
- 5.1.8. exigir da Contratada o fiel cumprimento das obrigações decorrentes desta contratação; e
- 5.1.9. verificar a manutenção pela contratada das condições de habilitação estabelecidas na licitação.

5.2. São obrigações da Contratada:

- 5.2.1. prestar ao CIM os serviços objeto desta contratação, conforme estabelecido neste TR, no Edital de Licitação e nos demais anexos, obedecendo à regulamentação aplicável;
- 5.2.2. fornecer o Suporte Técnico durante toda a vigência da contratação, por meio de chamada telefônica, sistema próprio de atendimento ou e-mail, sem nenhum ônus ao CIM, a fim de que seja possível registrar reclamações sobre o funcionamento do serviço contratado, obter suporte técnico e esclarecimentos;
- 5.2.3. assumir inteira responsabilidade técnica e administrativa sobre o objeto contratado, não podendo transferir a outras empresas a responsabilidade por problemas de funcionamento do serviço. A Fiscalização não aceitará a transferência de qualquer responsabilidade da Contratada para terceiros;
- 5.2.4. responsabilizar-se pelas infrações à regulamentação aplicável ao objeto da contratação, que consistirão em infrações contratuais quando comprometerem os serviços prestados ao CIM;
- 5.2.5. manter, durante todo o prazo de execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na fase de habilitação da licitação;
- 5.2.6. aceitar, nas mesmas condições contratuais, os acréscimos ou supressões nos serviços, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato, que se fizerem necessários, nos termos do artigo 125 da Lei 14.133/21;
- 5.2.7. receber os valores que lhe forem devidos pelo pela prestação dos serviços, na forma disposta neste TR;
- 5.2.8. abster-se de praticar atos ilícitos, em especial os descritos no art. 5º da Lei Federal nº 12.846, de 2013;
- 5.2.9. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do Contrato;
- 5.2.10. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- 5.2.11. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não

excluindo ou reduzindo a responsabilidade da Fiscalização ou o acompanhamento da execução dos serviços pela Contratante;

- 5.2.12. propiciar todos os meios necessários à Fiscalização do Contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
- 5.2.13. quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução;
- 5.2.14. quando especificado, manter a disponibilidade mínima de fornecimento da solução durante a execução do Contrato; e
- 5.2.15. fazer a transição contratual, quando for o caso.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Condições de execução

6.2. A execução do objeto seguirá a seguinte dinâmica:

- 6.2.1. Início da execução do objeto: em até 30 (trinta) dias da assinatura do Contrato;

6.3. Rotinas de execução

- 6.4. O fornecedor será selecionado mediante pregão eletrônico;
- 6.5. Uma orientação inicial sobre utilização da solução deverá ocorrer dentro do prazo de homologação e aceite da solução;
- 6.6. A Contratada deverá realizar o acompanhamento da operação inicial da solução pelo período de 15 (quinze) dias, com o objetivo prestar o Suporte Técnico necessário (incluindo ajustes porventura identificados) para que a operação ocorra de forma controlada e segura;
- 6.7. A prestação do serviço descrito no objeto deverá ter seu horário de fornecimento de 24 horas por dia, durante 7 (sete) dias por semana, de forma ininterrupta, independentemente de feriados locais ou nacionais;
- 6.8. A Contratante deverá designar a Equipe de Fiscalização da Contratação que será a responsável pela gestão da Solução pela Contratante;
- 6.9. A Contratada deverá designar um Gestor do Contrato, que deverá fazer acompanhamento de seu desempenho junto à Contratante;
- 6.10. A Contratada deverá manter a capacidade de Suporte Técnico e de manutenção durante a vigência do Contrato; e
- 6.11. Quaisquer desvios ou situações que possam vir a comprometer a execução, objetivos e resultados esperados deverão ser formalizados entre as partes por escrito, e devidamente registrados pela Contratante.
- 6.12. **Local e horário da prestação dos serviços**
- 6.13. Os serviços serão prestados ao CIM, sendo acessíveis de qualquer computador conectado à Internet, em território nacional, por se tratar de uma solução que opera na modalidade “Software como Serviço” (SaaS).
- 6.14. O serviço prestado por meio da solução de gestão de risco cibernético deverá estar disponível 24 horas por dia, 7 dias por semana, ao longo de toda a extensão do Contrato.

6.15. Materiais a serem disponibilizados

6.16. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais necessários à instrução sobre o funcionamento da solução, conforme a modalidade em que for ministrada.

6.17. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

6.18. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

6.19. Formas de transferência de conhecimento

6.20. Não será necessária transferência de conhecimento devido às características do objeto.

6.21. Procedimentos de transição e finalização do Contrato

6.22. Não serão necessários procedimentos de transição e finalização do Contrato devido às características do objeto.

6.23. Quantidade mínima de serviços para comparação e controle

6.24. As quantidades mínimas de bens ou serviços para comparação e controle são as mesmas descritas no item “Descrição do Bem ou Serviço” deste TR.

6.25. Mecanismos formais de comunicação

6.26. São definidos como mecanismos formais de comunicação, entre a Contratante e a Contratada, os seguintes:

6.26.1. Ordem de Serviço;

6.26.2. Ata de Reunião;

6.26.3. Ofício;

6.26.4. Sistema de abertura de chamados;

6.26.5. E-mail; e

6.26.6. Carta.

6.27. Formas de Pagamento

6.28. Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio do Modelo de Gestão do Contrato.

6.29. Manutenção de Sigilo e Normas de Segurança

6.30. O Contratado 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 dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.31. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, encontra-se no Anexo II.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O Contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

- 7.2. Em caso de impedimento, ordem de paralisação ou suspensão do Contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.
- 7.3. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
- 7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.
- 7.5. Preposto**
- 7.6. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.
- 7.7. A Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade
- 7.8. Reunião Inicial**
- 7.9. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.
- 7.10. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 15 (quinze) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.
- 7.10.1. A reunião poderá ser realizada nas modalidades presencial ou à distância, por meio de plataforma online (Zoom, Cisco Webex, Microsoft Teams, Google Meet).
- 7.10.2. A pauta desta reunião observará, pelo menos:
- 7.10.2.1. Participação do representante legal da Contratada, que apresentará o seu preposto;
- 7.10.2.2. Entrega, por parte da Contratada, do Termo de Compromisso e Manutenção do Sigilo;
- 7.10.2.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do Contrato;
- 7.10.2.4. Apresentação das declarações/certificados do desenvolvedor da solução, comprovando que o serviço ofertado possui a garantia solicitada neste TR.
- 7.11. Fiscalização**
- 7.12. A execução do Contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do Contrato, ou pelos respectivos substitutos ([Lei nº 14.133, de 2021, art. 117, caput](#)) , nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.
- 7.13. Fiscalização Técnica**
- 7.14. O fiscal técnico do Contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do Contrato, para que sejam cumpridas todas as condições estabelecidas no Contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI).
- 7.15. O fiscal técnico do Contrato anotará no histórico de gerenciamento do Contrato todas as ocorrências relacionadas à execução do Contrato, com a descrição do que for necessário para a regularização

das faltas ou dos defeitos observados. ([Lei nº 14.133, de 2021, art. 117, §1º](#), e [Decreto nº 11.246, de 2022, art. 22, II](#)).

- 7.16. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do Contrato emitirá notificações para a correção da execução do Contrato, determinando prazo para a correção. ([Decreto nº 11.246, de 2022, art. 22, III](#)).
- 7.17. O fiscal técnico do Contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. ([Decreto nº 11.246, de 2022, art. 22, IV](#)).
- 7.18. No caso de ocorrências que possam inviabilizar a execução do Contrato nas datas aprezadas, o fiscal técnico do Contrato comunicará o fato imediatamente ao gestor do Contrato. ([Decreto nº 11.246, de 2022, art. 22, V](#)).
- 7.19. O fiscal técnico do Contrato comunicará ao gestor do Contrato, em tempo hábil, o término do Contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual ([Decreto nº 11.246, de 2022, art. 22, VII](#)).

7.20. Fiscalização Administrativa

- 7.21. O fiscal administrativo do Contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário ([Art. 23, I e II, do Decreto nº 11.246, de 2022](#)).
- 7.21.1. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do Contrato atuará tempestivamente na solução do problema, reportando ao gestor do Contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; ([Decreto nº 11.246, de 2022, art. 23, IV](#)).
- 7.22. Além do disposto acima, a Fiscalização contratual obedecerá à(s) seguinte(s) rotina(s):
- 7.22.1. Verificação, a cada período de 30 dias, a contar do início do provimento do serviço, do índice de disponibilidade (ID) da solução, a fim de acompanhar se a prestação do serviço tem apresentado o nível estabelecido nos requisitos deste TR.

7.23. Gestor do Contrato

- 7.24. O gestor do Contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e Fiscalização do Contrato contendo todos os registros formais da execução no histórico de gerenciamento do Contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do Contrato para fins de atendimento da finalidade da administração. ([Decreto nº 11.246, de 2022, art. 21, IV](#)).
- 7.25. O gestor do Contrato acompanhará os registros realizados pelos fiscais do Contrato, de todas as ocorrências relacionadas à execução do Contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassem a sua competência. ([Decreto nº 11.246, de 2022, art. 21, II](#)).
- 7.26. O gestor do Contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. ([Decreto nº 11.246, de 2022, art. 21, III](#)).

- 7.27. O gestor do Contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. ([Decreto nº 11.246, de 2022, art. 21, VIII](#)).
- 7.28. O gestor do Contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. ([Decreto nº 11.246, de 2022, art. 21, X](#)).
- 7.29. O gestor do Contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. ([Decreto nº 11.246, de 2022, art. 21, VI](#)).
- 7.30. O gestor do Contrato deverá enviar a documentação pertinente ao setor de Contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela Fiscalização e gestão nos termos do Contrato.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

- 8.1. O pagamento será realizado em cota única no Recebimento Definitivo da solução.
- 8.2. A avaliação da execução do objeto ocorrerá durante todo o Contrato, cuja mensuração se dará em períodos de 30 (trinta) dias, a contar do início do provimento do serviço.
- 8.3. Será utilizado o Instrumento denominado Índice de Disponibilidade (ID), de responsabilidade de acompanhamento pela Fiscalização do Contrato, conforme o disposto a seguir:
- 8.3.1. A quantidade de dias que a solução estava integralmente disponível para acesso, sem intercorrências ou ausências de suas funcionalidades especificadas neste TR; e
- 8.3.2. A performance adequada com que as informações consultadas eram disponibilizadas, com o fito de atender à demanda de um analista em pleno uso da solução.
- 8.4. A disponibilidade do serviço (ds) será de observação diária pela Contratante, de modo que os itens “8.3.1” e “8.3.2” sejam atendidos.
- 8.5. O cômputo do indicador de disponibilidade do serviço será a cada 30 (trinta) dias, considerando a quantidade de dias indisponíveis (di) e a quantidade de dias de disponibilidade (dd) do serviço no período de referência.

$$ds = \frac{dd - di}{dd}$$

- 8.6. O cálculo pode ser observado na fórmula a seguir:
- 8.7. O indicador de disponibilidade do serviço deverá ser observado a cada período e pela Contratante e pela Contratada, de maneira que seja igual ou superior a 93,34%, o que corresponde, aproximadamente, a 2 (dois) dias de indisponibilidade toleráveis no espaço de 30 (trinta) dias.
- 8.8. **Do recebimento**
- 8.9. Os serviços serão recebidos provisoriamente, no prazo de 10 (dez) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. ([Art. 140, I, a, da Lei nº 14.133](#) e [Arts. 22, X e 23, X do Decreto nº 11.246, de 2022](#)).

- 8.9.1.** O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda da Contratada com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.
- 8.10.** O fiscal técnico do Contrato realizará o recebimento provisório do objeto do Contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. ([Art. 22, X, Decreto nº 11.246, de 2022](#)).
- 8.11.** O fiscal administrativo do Contrato realizará o recebimento provisório do objeto do Contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. ([Art. 23, X, Decreto nº 11.246, de 2022](#))
- 8.12.** O fiscal setorial do Contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.
- 8.13.** O recebimento provisório também ficará sujeito à conclusão de todos os testes de campo e à realização da instrução inicial de utilização da solução.
- 8.14.** Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste TR e na proposta, sem prejuízo da aplicação das penalidades.
- 8.15.** Quando a Fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do Contrato, em relação à Fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do Contrato para recebimento definitivo.
- 8.16.** Os serviços serão recebidos definitivamente no prazo de 20 (vinte) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e a consequente aceitação mediante termo detalhado, obedecendo aos seguintes procedimentos:
- 8.16.1.** Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento ([art. 21, VIII, Decreto nº 11.246, de 2022](#)).
- 8.16.2.** Realizar a análise dos relatórios e de toda a documentação apresentada pela Fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;
- 8.16.3.** Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e
- 8.16.4.** Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela Fiscalização.
- 8.16.5.** Enviar a documentação pertinente ao setor de Contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela Fiscalização e gestão.
- 8.17.** No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do [art. 143 da Lei nº 14.133, de 2021](#), comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.
- 8.18.** Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela Contratada, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.19. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do Contrato.

8.20. Procedimentos de Teste e Inspeção

8.21. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

8.21.1. Acesso online à solução, em caráter de experimentação, para verificação e validação do atendimento aos requisitos dispostos neste TR;

8.21.2. Avaliação da eficácia da instrução inicial (treinamento) para utilização da solução; e

8.21.3. Contato, em caráter de teste, com os canais de Suporte Técnico.

8.22. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

8.23. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 24 (vinte e quatro) horas úteis.	- Notificação; - Advertência; ou - Multa de 01 (um) % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 5 (cinco) dias úteis. Após o limite de 5 (cinco) dias úteis, aplicar-se-á multa de 5 (cinco) % do valor total do Contrato.
2	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	- Notificação; - Advertência; ou - Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 01 (um) % do valor total do Contrato.

8.24. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que a Contratada:

8.24.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.24.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8.25. Liquidação

8.26. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 30 (trinta) dias para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do [art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022](#).

8.27. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

- 8.28.** Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:
- 8.28.1.** o prazo de validade;
 - 8.28.2.** a data da emissão;
 - 8.28.3.** os dados do Contrato e do órgão Contratante;
 - 8.28.4.** o período respectivo de execução do Contrato;
 - 8.28.5.** o valor a pagar; e
 - 8.28.6.** eventual destaque do valor de retenções tributárias cabíveis.
- 8.29.** Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;
- 8.30.** A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.
- 8.31.** A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas. (Instrução Normativa nº 3, de 26 de abril de 2018).
- 8.32.** Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.
- 8.33.** Não havendo regularização ou sendo a defesa considerada improcedente, a Contratante deverá comunicar aos órgãos responsáveis pela Fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 8.34.** Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.
- 8.35.** Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso o contratado não regularize sua situação junto ao SICAF.
- 8.36. Prazo de pagamento**
- 8.37.** O pagamento será efetuado no prazo de até 30 (trinta) dias contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.
- 8.38.** No caso de atraso pela Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IGPM de correção monetária.
- 8.39. Forma de pagamento**

- 8.40. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.
- 8.41. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 8.42. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 8.43. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.
- 8.44. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.
- 8.45. Antecipação de pagamento**
- 8.46. A presente contratação permite a antecipação do pagamento total, conforme as regras previstas no presente tópico.
- 8.47. A Contratada emitirá nota fiscal correspondente ao valor da antecipação de pagamento, tão logo seja assinado o termo de Contrato, para que a Contratante efetue o pagamento antecipado.
- 8.48. Fica a Contratada obrigada a devolver, com correção monetária, a integralidade do valor antecipado na hipótese de inexecução do objeto.
- 8.49. No caso de inexecução parcial, deverá haver a devolução do valor proporcional ao tempo não-executada do Contrato.
- 8.50. O valor antecipado e não executado do Contrato será atualizado monetariamente pela variação acumulada do IGPM, ou outro índice que venha a substituí-lo, desde a data do pagamento da antecipação até a data da devolução.
- 8.51. A liquidação ocorrerá de acordo com as regras do tópico respectivo deste instrumento.
- 8.52. O pagamento antecipado será efetuado no prazo máximo de até 15 (quinze) dias, contados do recebimento da nota fiscal, a critério da Administração Naval.
- 8.53. A antecipação de pagamento dispensa o ateste ou recebimento prévios do objeto, os quais deverão ocorrer após a regular execução contratual a que se refere o valor antecipado.
- 8.54. O pagamento de que trata este item está condicionado à tomada das seguintes providências pela Contratada:
- 8.54.1. realização da reunião inicial entre representantes da Contratante e da Contratada;
- 8.54.2. comprovação de início da execução do objeto pelo Contratada, para a antecipação do valor; e
- 8.54.3. comprovação de que foi ministrada a instrução inicial de utilização da solução.
- 8.55. O pagamento do valor a ser antecipado ocorrerá respeitando eventuais retenções tributárias incidentes.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

9.1. Forma de seleção e critério de julgamento da proposta

9.2. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

9.3. Regime de execução

9.4. O regime de execução do Contrato será por fornecimento e prestação de serviço associado.

9.5. Da Aplicação da Margem de Preferência

9.6. Não se vislumbra a aplicabilidade da margem de preferência ao objeto em tela.

9.7. Exigências de habilitação

9.8. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

9.9. Habilitação jurídica

9.9.1. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

9.9.2. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.9.3. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

9.9.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou Contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

9.9.5. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução [Normativa DREI/ME nº 77, de 18 de março de 2020](#).

9.9.6. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

9.9.7. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

9.9.8. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembléia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o [art. 107 da Lei nº 5.764, de 16 de dezembro 1971](#).

9.10. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.11. Habilitação fiscal, social e trabalhista

9.11.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

- 9.11.2.** Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradoria-Geral da Fazenda Nacional;
- 9.11.3.** Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- 9.11.4.** Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;
- 9.11.5.** Prova de inscrição no cadastro de contribuintes Estadual/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- 9.11.6.** Prova de regularidade com a Fazenda Estadual/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- 9.11.7.** Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei; e
- 9.11.8.** O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

9.12. Qualificação Econômico-Financeira

- 9.12.1.** Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;
- 9.12.2.** Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);
- 9.12.3.** Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:
 - 9.12.3.1.** Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);
 - 9.12.3.2.** As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e
 - 9.12.3.3.** Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.
- 9.12.4.** Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.
- 9.12.5.** Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo de até 10 (dez) % do valor total estimado da contratação.

- 9.12.6.** As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).
- 9.12.7.** O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

9.13. Qualificação Técnica

- 9.13.1.** Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação;
- 9.13.1.1. A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação
- 9.13.2.** Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.
- 9.13.3.** Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- 9.13.4.** Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 9.13.5.** O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do Contrato que deu suporte à contratação, endereço atual da Contratante e local em que foi executado o objeto contratado, dentre outros documentos.
- 9.13.6.** Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:
- 9.13.6.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o Contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;
- 9.13.6.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;
- 9.13.6.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;
- 9.13.6.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;
- 9.13.6.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o Contrato;
- 9.13.6.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o Contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação; e

- 9.13.6.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

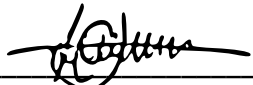
- 10.1. O custo estimado total da contratação é de R\$ 180.000,00 (cento e oitenta mil reais).
- 10.2. Em caso de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:
- 10.2.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na linha "d" do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;
- 10.2.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;
- 10.2.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou
- 10.2.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

11. ADEQUAÇÃO ORÇAMENTÁRIA

- 11.1. A indicação da dotação orçamentária fica postergada para o momento da assinatura do Contrato ou instrumento equivalente.

11.2. Cronograma Físico Financeiro

Evento	Prazo estimado	Valor
Serviço de provimento da solução de gestão de risco cibernético.	30 (trinta) dias após a emissão da Nota Fiscal	R\$ 180.000,00
Treinamento	5 (cinco) dias após a assinatura do Contrato	N/A
Suporte Técnico	5 (cinco) dias após a assinatura do Contrato	N/A

 Integrante Requisitante CT(T) Mauricio Fulginiti Olivaes Munhoz Encarregado da Divisão de Inteligência Cibernética NIP: 09.0022.01	 Integrante Técnico CF Flávio de Queiroz Guimarães Chefe do Departamento de Atividades Cibernéticas NIP: 87.3012.11	 Integrante Administrativo CF(IM) Leonardo Barbosa da Silva Chefe do Departamento de Administração NIP: 96.0305.42
--	--	---

