MF-CVM-COMISSAO DE VALORES MOBILIARIOS/RJ

Estudo Técnico Preliminar 64/2025

1. Informações Básicas

Número do processo: 19957.000460/2026-12

2. Descrição da necessidade

Serviço Gerenciado de Segurança - MSS

1. O presente estudo visa estabelecer os detalhes técnicos e contratuais para a manutenção e melhoria dos Serviços Gerenciados de Segurança (MSS - Managed Security Services) disponíveis na CVM desde 2021, data da primeira contratação dos serviços.

2. A complexidade do cenário de ameaças no ambiente computacional das organizações, e da CVM em particular, evoluiu de forma significativa nos últimos anos. Ataques mais rápidos, automatizados e difíceis de detectar colocam em risco informações sensíveis sob responsabilidade da autarquia. A simples existência de normas, diretrizes e comitês não garante proteção suficiente. Hoje, segurança exige capacidade operacional contínua, resposta rápida e visibilidade completa do ambiente.

3. Dessa forma, a implementação de controles, sua monitoração contínua e a correta tratativa de incidentes só se sustentam com ferramentas adequadas e serviços especializados. A ausência de *enforcement* e acompanhamento estruturado resulta em falhas, exposição prolongada a riscos e respostas reativas — um cenário incompatível com a criticidade das informações tratadas pela CVM.

4. Além disso, o quadro atual da equipe interna não permite a dedicação integral necessária para lidar com a sofisticação dos ataques contemporâneos, nem suporta mais o rastreio e o tratamento manual de prevenção, identificação e tratamento de incidentes de segurança. Não se trata apenas de aumentar esforço: é uma questão de capacidade técnica, escala operacional e disponibilidade 24/7, algo que equipes reduzidas não conseguem prover, especialmente diante da escalada de incidentes registrados nos setores público e privado.

5. É necessário considerar que os prejuízos decorrentes de vazamentos, indisponibilidade ou manipulação de informações superam, com ampla margem, o custo de serviços especializados. Além do impacto financeiro e operacional, há riscos de danos à imagem institucional e de perda de confiança por parte do mercado e da sociedade. Ignorar essa realidade é aceitar a inevitabilidade de incidentes com consequências potencialmente graves.

6. Para corroborar com essa necessidade, os órgãos de controle aos quais a CVM responde têm exigido cada vez mais e melhores ações de controle e de mitigação de riscos de segurança da informação dos órgãos do SISP, que a autarquia faz parte, o que requer a evolução dos serviços para o atendimento das medidas classificadas como prioritárias no Programa de Privacidade e Segurança da Informação - PPSI, conduzido pela Secretaria de Governo Digital (SGD), vinculada ao Ministério da Gestão e da Inovação em Serviços Públicos (MGI).

7. Diante disso, a contratação de serviços gerenciados de segurança — executados por empresa especializada, com equipe dedicada, ferramentas consolidadas e operação contínua — torna-se a medida mais eficaz para reduzir riscos, fortalecer a postura de segurança da CVM e suprir de imediato as lacunas operacionais existentes. Trata-se de uma necessidade estratégica, não de uma conveniência.

8. Diante do exposto, atesta-se a essencialidade e o relevante interesse público desta contratação, em observância ao disposto no art. 3º do Decreto nº 8.540/2015.

3. Área requisitante

Área Requisitante	Responsável
Superintendência de Tecnologia da Informação - STI	Gustavo Henrique Gori Maia

4. Necessidades de Negócio

1. Requisitos gerais

1.1. Reduzir as vulnerabilidades de Segurança da Informação (SI) do ambiente da CVM demanda um processo contínuo de identificação, priorização e correção de falhas, garantindo que os controles técnicos e procedimentais acompanhem a maturidade necessária para proteger informações sensíveis.

1.2. Tratar adequadamente os incidentes de SI exige capacidade de detecção ágil, análise especializada e respostas coordenadas, assegurando contenção rápida, mitigação de impactos e comunicação estruturada aos envolvidos, reduzindo riscos operacionais e reputacionais.

1.3. Monitorar a utilização dos recursos e sistemas críticos, sob o aspecto de SI, é fundamental para identificar comportamentos anômalos, prevenir acessos indevidos e antecipar potenciais ameaças, permitindo decisões rápidas e baseadas em evidências.

1.4. Assegurar conformidade com normas e regulamentações aplicáveis — como ISO 27001, LGPD e diretrizes internas — torna-se um requisito de negócio essencial para garantir que os processos de segurança estejam alinhados às obrigações institucionais, fortalecer a governança e o atendimento aos requisitos de conformidade, bem como evitar eventuais penalidades.

1.5. Ampliar a capacidade de resposta e resiliência operacional frente a incidentes, garantindo continuidade dos serviços essenciais da autarquia, constitui uma necessidade estratégica, já que a indisponibilidade de sistemas críticos pode comprometer diretamente sua missão institucional.

1.6. Viabilizar a implementação das medidas elencadas como prioritárias no Programa de Privacidade e Segurança da Informação - PPSI, coordenado pela Secretaria de Governo Digital - SGD, subordinada ao Ministério da Gestão e da Inovação em Serviços Públicos - MGI.

2. Alinhamento ao Plano Diretor de Logística Sustentável (PLS)

2.1 A presente contratação encontra-se alinhada ao Plano Diretor de Logística Sustentável (PLS) da CVM, na medida em que incorpora critérios e práticas de sustentabilidade compatíveis com as diretrizes institucionais de uso racional de recursos, eficiência operacional e mitigação de impactos ambientais, conforme previsto no referido instrumento.

5. Necessidades Tecnológicas

1. Disponibilizar ferramentas amplamente reconhecidas no mercado, capazes de sustentar os processos internos de segurança da informação da CVM e fornecer subsídios técnicos adequados para a tomada de decisão pela equipe da autarquia.

2. Promover a redução de vulnerabilidades técnicas por meio da identificação sistemática de riscos, da orientação quanto às ações corretivas necessárias e do monitoramento contínuo das fragilidades presentes nas ferramentas e sistemas utilizados pela autarquia.

3. Permitir a coleta, retenção histórica e análise estruturada de logs dos sistemas e ferramentas da CVM, de forma a identificar tentativas de acesso indevido, comportamentos atípicos ou possíveis indícios de comprometimento.

4. Aprimorar as ações de conscientização dos usuários, elevando o nível de percepção sobre riscos técnicos, cibernéticos, ameaças de engenharia social e práticas inadequadas de compartilhamento de informações pessoais ou corporativas.

5. Assegurar que a proteção dos endpoints se mantenha em níveis equivalentes ou superiores aos atualmente alcançados, garantindo atualização contínua das capacidades de defesa e de resposta.

6. Monitorar o ambiente externo da CVM para identificar riscos relacionados à imagem institucional, possíveis exposições de informações corporativas e sinais de coordenação de ataques direcionados à autarquia.

7. Fortalecer a governança de segurança da informação, garantindo alinhamento às normas e boas práticas aplicáveis, como ISO 27001, LGPD e diretrizes internas, promovendo maior maturidade e previsibilidade nos processos de gestão de riscos.

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

1. Requisitos de Licenciamento

1.1. As ferramentas de software fornecidas para compor a solução deverão ser de propriedade da CONTRATADA por meio de licenciamento junto ao fabricante e deverão ser suficientes para permitir a plena operacionalização das funcionalidades necessárias para atender ao contrato.

1.2. Tais ferramentas deverão possuir suporte do fabricante e não poderão ser entregues por meio de software livre, open source ou INHOUSE.

1.3. Deve ser possível realizar a ampliação e o remanejamento de licenças dentro do escopo de cada serviço contratado, de acordo com a demanda da autarquia, conforme previsto na especificação técnica (vide Anexo ETP.I - Especificação Técnica da Solução).

1.4. No caso específico do serviço de Gestão de Vulnerabilidades, a CVM utiliza a ferramenta Tenable One, conforme previsto na especificação técnica (vide Anexo ETP.I - Especificação Técnica da Solução).

2. Requisitos de Capacitação

2.1. Serão previstos treinamentos para capacitação da equipe técnica da CVM nas principais ferramentas ofertadas, a fim de prover autonomia na utilização e permitir a solicitação de demandas à CONTRATADA mais claras e objetivas, além de facilitar as atividades de gestão técnica da contratação. Os requisitos mínimos para os treinamentos, em cada solução, são os seguintes:

2.2. Treinamento em gestão de vulnerabilidades, cujo detalhamento está apresentado no item 2.4. TREINAMENTO EM GESTÃO DE VULNERABILIDADES, do Anexo ETP.I - Especificação Técnica da Solução.

2.3. Treinamento em monitoramento e resposta a incidentes cibernéticos, cujo detalhamento está apresentado no item 3.3. TREINAMENTO EM MONITORAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS do Anexo ETP.I - Especificação Técnica da Solução.

2.4. Treinamento em inteligência de ameaças cibernéticas, cujo detalhamento está apresentado no item 4.12. TREINAMENTO EM INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS do Anexo ETP.I - Especificação Técnica da Solução.

2.5. Treinamento em proteção de endpoints, cujo detalhamento está apresentado no item 5.7. TREINAMENTO EM PROTEÇÃO DE ENDPOINTS do Anexo ETP.I - Especificação Técnica da Solução.

3. Requisitos de Manutenção

3.1. A CONTRATADA deverá disponibilizar canal único de sistema para abertura de chamados para suporte e manutenção via Web, e-mail e telefone.

3.2. A CONTRATADA deverá fornecer todas as atualizações e novas versões dos softwares constantes da solução lançadas durante a vigência do contrato, sem ônus para a CVM.

3.3. As obrigações de manutenção (*software subscription*) deverão incluir atualizações de versões e pequenas atualizações de release, além de reparos de defeitos pontuais (*bug fixing patches*), assim que forem lançados no mercado.

3.4. Equipamentos disponibilizados pela CONTRATADA no ambiente da CVM, para a sustentação dos serviços, deverão contar com garantia e suporte às expensas da CONTRATADA, durante a vigência contratual.

3.5. Manutenções corretivas deverão ser executadas pela CONTRATADA onde os equipamentos estiverem instalados (on-site), mediante anuência e alinhamento com a equipe técnica da CVM para a definição da janela de indisponibilidade.

3.6. Na data do certame licitatório, nenhuma das ferramentas/soluções que compõem os serviços oferecidos poderá estar/ser listada no site oficial do fabricante em listas de end-of-sale, end-of-support, end-of-life ou similares.

3.7. As ferramentas/soluções que compõem os serviços oferecidos deverão ser atualizáveis durante todo o período do contrato. Caso alguma das ferramentas/soluções entre em processo de descontinuação, a CONTRATADA deverá promover a substituição imediata da ferramenta/solução por outra equivalente, sem ônus para a CONTRATANTE.

4. Requisitos Temporais

4.1. A CONTRATADA deverá finalizar a implantação e a migração dos dados das soluções atuais em, no máximo, 45 (quarenta e cinco) dias corridos, a contar da data de assinatura do contrato, a seu ônus e responsabilidade, com entrega de todos os itens necessários à execução dos serviços descritos neste documento.

4.2. A CONTRATADA deverá obedecer aos prazos de atendimento das demandas da CVM de acordo com o previsto no **Anexo ETP.II - Nota Técnica de Nível de Serviço**.

5 Requisitos de Segurança da Informação

5.1. A CONTRATADA deverá assinar os Termos de Ciência e Termo de Compromisso e Manutenção de Sigilo a ser obedecido por ela e seus funcionários.

5.2. Não será permitida a divulgação, sob nenhuma hipótese, de qualquer documento associado à contratação ou à CVM, confidencial ou não, sem prévia permissão da CVM.

5.3. Observar as diretrizes de Segurança da Informação e Privacidade (SIP) conforme Seção 7 do ANEXO I da IN SGD/ME nº 94/2022 e a legislação vigente.

5.4. Manter conformidade com a Lei nº 13.709/2018 (LGPD) e legislação vigente para dados pessoais e informações classificadas.

5.5. A CONTRATADA deverá adequar o ambiente tecnológico fornecido à CVM sempre que novas políticas de segurança da informação da autarquia sejam criadas ou modificadas. Tais diretrizes podem ser encontradas na **PORTARIA CVM/PTE/Nº 155, DE 31 DE AGOSTO DE 2021**. As adequações serão sempre demandadas pela equipe técnica da Superintendência de Tecnologia da Informação (STI) em conjunto com a CONTRATADA.

5.6. A CONTRATADA deverá adotar controles e métodos presentes na norma ISO 27001.

6 Requisitos de Arquitetura Tecnológica

6.1. A CONTRATADA do serviço de SOC deverá possuir espaço físico com características que aumentem sua disponibilidade, resiliência e segurança de acesso.

6.2. A CONTRATADA será a responsável por fornecer todas as ferramentas e licenças para a prestação do serviço, exceto quando explicitamente definido o contrário.

6.3. A comunicação entre os ambientes da CVM e da CONTRATADA será feita por VPN *site-to-site*, não sendo necessário link dedicado.

7 Requisitos de Implantação

7.1. A CONTRATADA deverá desenvolver e apresentar um macro cronograma de implantação, além de definir estratégia de implantação, em conjunto com a equipe técnica da CVM.

7.2. Este macro cronograma deverá ser apresentado na reunião inicial (*kickoff*) com a equipe técnica da CVM, de forma a definir um cronograma detalhado de execução.

7.3. Durante o projeto, a CONTRATADA deverá realizar interação frequente com os profissionais da CVM com vistas à transferência do conhecimento aplicado, desde os estudos iniciais, até a migração e a concretização da implantação.

7.4. Questionamentos e demandas encaminhadas pela CVM à CONTRATADA deverão ser respondidas tempestivamente por esta.

7.5. A CONTRATADA é responsável pela instalação completa e configuração dos equipamentos e respectivos *softwares* garantindo que estes estejam operacionais e otimizados para o ambiente da CVM.

7.6. A CONTRATADA deverá realizar uma avaliação preliminar do ambiente computacional da CVM, considerando a arquitetura da infraestrutura atual de forma a identificar quaisquer pré-requisitos e possíveis necessidades técnicas.

7.7. Para fins de documentação, a CONTRATADA deverá entregar um Plano de Projeto, contendo, no mínimo, os artefatos: Termo de Abertura, Declaração de Escopo, Matriz RACI, Cronograma com *milestones* e Recursos Humanos.

7.8. Para fins de migração, a CONTRATADA deverá fornecer documentos técnicos em cada etapa do projeto. Exemplos incluem as documentações técnicas referentes a configurações aplicadas, desenhos de arquitetura, baselines, controles técnicos, dentre outros.

7.9. A implantação não deve interromper as operações diárias da CVM e deve ser feita de forma a minimizar o tempo de inatividade.

7.10. A CONTRATADA é responsável por quaisquer materiais ou softwares para a implantação do serviço.

7.11. A implantação poderá englobar as seguintes atividades:

7.11.1. Instalação física e lógica:

a. A instalação ocorrerá em rack nas localidades da CONTRATANTE. A fixação ocorrerá por meio de conjunto a ser fornecido com o equipamento, também pela CONTRATADA, quando aplicável.

7.11.2. Configuração

a. Nesta etapa, os controles técnicos em produção e quaisquer configurações legadas deverão ser migradas para as novas soluções, além de criação de novas regras e políticas que se mostrarem necessárias.
b. Os softwares e equipamentos devem ser configurados em sua última versão estável com seus patches (*releases*) mais recentes instalados. Não serão aceitas funcionalidades que estejam executando em *builds* não estáveis (alpha, beta etc.) ou modificações personalizadas diretamente em código.

7.11.3. Testes

a. A CONTRATADA deverá fornecer documentação técnica que comprove o funcionamento de TODAS as funcionalidades implementadas. A documentação deverá conter, pelo menos, a descrição da funcionalidade testada e o roteiro de testes com o respectivo resultado de modo que o teste possa ser reproduzível pela CVM.

7. Estimativa da demanda - quantidade de bens e serviços

1. Tabela de serviços - Modelo de Contratação

Grupo	Item	Descrição	Subitem	Serviço	CATSER	Métrica	Volume (Inicial / Máximo)
1	1	Gestão de Vulnerabilidades	1.1	Licenças de software	27502	Unidade/mês	500 / 2000
			1.2	Serviço de administração	27014	Mês	36
			1.3	Treinamento	3840	Unidade	2
	2	Monitoramento e resposta a incidentes	2.1	Ferramentas de monitoramento	27502	Mês	36
			2.2	Serviço de administração	27014	Mês	36
			2.3	Treinamento	3840	Unidade	2
	3	Inteligência de ameaças cibernéticas	3.1	Serviço de administração	27014	Mês	36
			3.2	Takedowns	27014	Unidades	180
			3.3	Treinamento	3840	Unidade	2
2	4	Proteção de endpoints	4.1	Licenças de software	27502	Unidades/mês	800 / 1000
			4.2	Serviço de administração	27014	Mês	36
			4.3	Treinamento	3840	Unidade	2
3	5	Conscientização em segurança da informação	5.1	Licenças de uso	27502	Unidade/mês	200 / 800
			5.2	Serviço de implantação	26972	Pgto. Único	1
			5.3	Consultoria Técnica	27340	Horas	240
4	6	Testes de invasão	6.1	Execução de pentest	27014	Unidades	12

**As referências de CATMAT e CATSER acima compreendem apenas uma referência considerando compras da administração pública.*

1.1. Item 1 - Gestão de vulnerabilidades

- Especificação: Conforme detalhamento apresentado no capítulo 2 do **Anexo TR.I - Especificação Técnica da Solução**.
- Motivação Técnica: Identificar possíveis vulnerabilidades de segurança da informação na infraestrutura e nas aplicações da CVM, a fim de reduzir a superfície de ataques cibernéticos direcionados aos ativos da autarquia.
- Quantitativos
  - Subitem 1.1: 500 licenças iniciais, 2000 licenças máximas, com crescimento condicionado à formalização de ordem de serviço emitida pela equipe de fiscalização do contrato.
  - Subitem 1.2: Serviço de implantação, migração de dados e gerenciamento mensal das ferramentas, para a aplicação de patches de segurança e de funcionalidade, atendimento de requisitos e de demandas solicitadas pela CVM e sustentação da solução.
  - Subitem 1.3: Número máximo de turmas de treinamento para a equipe técnica da CVM nas ferramentas fornecidas pela CONTRATADA. Estimativa de duas turmas, sendo a primeira no início da implantação

dos serviços e a segunda para atender eventuais movimentações na equipe ao longo da execução do contrato, cujo pagamento será apenas mediante a prestação do serviço.

- Estimativa de volume: Ativos existentes no ambiente que serão objeto de controle pela ferramenta. Atualmente, a CVM conta com aproximadamente 900 usuários, 100 equipamentos servidores, 140 equipamentos de rede, 110, equipamentos IoT, 800 estações de trabalho e 50 aplicações web, cuja relação de item x número de licenças deverá compor a proposta técnica e comercial. Os volumes estimados são os apresentados no item 2.2.6 do **Anexo ETP.I - Especificação Técnica da Solução**.
- Adicionalmente, quantitativo mínimo está relacionado ao volume de uso atual no ambiente, que não abrange todos os ativos requeridos nessa nova contratação, o que justifica o incremento das licenças.

1.2. Item 2 - Monitoramento e resposta a incidentes

- Especificação: Conforme detalhamento apresentado no capítulo 3 do **Anexo ETP.I - Especificação Técnica da Solução**.
- Motivação Técnica: Garantir o monitoramento contínuo e ininterrupto de ameaças direcionadas à CVM, por meio do correlacionamento de logs e da detecção de comportamentos anômalos de usuários, aplicações, serviços e infraestrutura que possam gerar eventos de segurança da informação.
- Quantitativos
  - Subitem 2.1: 1500 ativos do parque tecnológico da CVM, ou equivalente em eventos por segundo (EPS) ou GB/dia (gigabytes por dia). Para essa equivalência, deve-se utilizar a proporção de bytes/evento descrita item 3.2.1.9 no **Anexo ETP.I - Especificação Técnica da Solução.**
  - Subitem 2.2: Serviço de implantação, migração de dados e gerenciamento mensal das ferramentas, para a aplicação de patches de segurança e de funcionalidade, atendimento de requisitos e de demandas solicitadas pela CVM e sustentação da solução.
  - Subitem 2.3: Número máximo de turmas de treinamento para a equipe técnica da CVM nas ferramentas fornecidas pela CONTRATADA. Estimativa de duas turmas, sendo a primeira no início da implantação dos serviços e a segunda para atender eventuais movimentações na equipe ao longo da execução do contrato, cujo pagamento será apenas mediante a prestação do serviço.
- Estimativa de volume: Ativos e serviços existentes no ambiente da CVM, cujo detalhamento das origens de logs são apresentadas no item 3.2.1.11 e Seção 8 do **Anexo ETP.I - Especificação Técnica da Solução**.

1.3. Item 3 - Inteligência de ameaças cibernéticas

- Especificação: Conforme detalhamento apresentado no capítulo 4 do **Anexo ETP.I - Especificação Técnica da Solução**.
- Motivação Técnica: verificar, prevenir e antecipar-se, com ações, às ameaças identificadas em fontes disponíveis na Internet, tanto as acessadas abertamente quanto as chamadas deep e dark web - em busca de potenciais ameaças cibernéticas à CONTRATANTE.
- Quantitativos
  - Subitem 3.1: Serviço de implantação e gerenciamento mensal das ferramentas, para a aplicação de patches de segurança e de funcionalidade, atendimento de requisitos e de demandas solicitadas pela CVM e sustentação da solução.
  - Subitem 3.2: 180 (cento e oitenta) takedowns máximos para a remoção de recursos maliciosos (como domínios, URLs, serviços, contas em redes sociais, dentre outros) na Internet que se passem por recursos válidos da CVM, cujo pagamento será apenas mediante a prestação do serviço.
  - Subitem 3.3: Número máximo de turmas de treinamento para a equipe técnica da CVM nas ferramentas fornecidas pela CONTRATADA. Estimativa de duas turmas, sendo a primeira no início da implantação dos serviços e a segunda para atender eventuais movimentações na equipe ao longo da execução do contrato, cujo pagamento será apenas mediante a prestação do serviço.
- Estimativa de volume: O volume foi estimado baseado no tamanho da equipe gerencial, com aproximadamente 100 pessoas de interesse, no número de endereços de e-mail utilizados (caixas licenciadas e compartilhadas), domínios atuais utilizados (seis domínios registrados no Registro.BR). Os demais requisitos estão apresentados no item 4.1 do **Anexo ETP.I - Especificação Técnica da Solução**.

- Nos casos de definição do número de empresas fornecedoras monitoradas e requisições de takedowns, não há histórico de uso, uma vez que o serviço não existe atualmente. No entanto, o serviço é pago por uso, não havendo obrigatoriedade de execução.

1.4. Item 4 - Proteção de endpoints

- Especificação: Conforme detalhamento apresentado no capítulo 5 do **Anexo ETP.I - Especificação Técnica da Solução**.
- Motivação Técnica: fornecer licenças e operar a solução de proteção em equipamentos corporativos do parque tecnológico da CVM.
- Quantitativos
    - Subitem 4.1: 800 endpoints iniciais, podendo ser ampliado para até 1000 licenças. O crescimento é condicionado à formalização de ordem de serviço emitida pela equipe de fiscalização do contrato.
    - Subitem 4.2: Serviço de implantação e gerenciamento mensal das ferramentas, para a aplicação de patches de segurança e de funcionalidade, atendimento de requisitos e de demandas solicitadas pela CVM e sustentação da solução.
    - Subitem 4.3: Número máximo de turmas de treinamento para a equipe técnica da CVM nas ferramentas fornecidas pela CONTRATADA. Estimativa de duas turmas, sendo a primeira no início da implantação dos serviços e a segunda para atender eventuais movimentações na equipe ao longo da execução do contrato, cujo pagamento será apenas mediante a prestação do serviço.
- Estimativa de volume: Baseada no volume de uso atual e no tamanho do parque de estações de trabalho, além de previsão de crescimento para o restante do parque de equipamentos (Datacenter e Nuvem Pública) e necessidades da força de trabalho.

1.5. Item 5 - Conscientização em segurança da informação

- Especificação: Conforme detalhamento apresentado no capítulo 6 do **Anexo ETP.I - Especificação Técnica da Solução**.
- Motivação Técnica: conscientização dos recursos humanos da CVM sobre a importância de seguir a política de segurança da informação e as normas complementares estabelecidas, capacitando-os nas boas práticas de segurança da informação no ambiente corporativo da CVM.
- Quantitativos
    - Subitem 5.1: Atendimento de 200 usuários iniciais, podendo chegar a 800 licenças. O crescimento é condicionado à formalização de ordem de serviço emitida pela equipe de fiscalização do contrato.
    - Subitem 5.2: Serviço único de implantação das ferramentas.
    - Subitem 5.3: Volume máximo de horas de consultoria para abranger o atendimento de novas demandas, como o desenho de treinamentos personalizados para a equipe da autarquia, cujo pagamento será apenas mediante a prestação do serviço.
- Estimativa de volume: Considerando a mudança de característica do serviço, a equipe de planejamento entende que a fase de implantação do serviço envolverá um conjunto menor de usuários (até 200), evoluindo para toda a força de trabalho atual e estimativa de crescimento. Consideramos também os treinamentos requeridos pelas demandas apresentadas pelo Plano de Privacidade e Segurança da Informação - PPSI.

1.6. Item 6 - Testes de invasão

- Especificação: Conforme detalhamento apresentado no capítulo 7 do **Anexo ETP.I - Especificação Técnica da Solução**.
- Motivação Técnica: identificar vulnerabilidades de segurança no ambiente interno e externo da CVM por meio de testes direcionados para a exploração de aplicações.
- Quantitativos
    - Subitem 6.1: Número máximo de testes de invasão previstos ao longo da execução do contrato (4 por ano). O pagamento será realizado apenas mediante prestação do serviço.

- Estimativa de volume: Baseado no histórico de utilização de serviços (1 por semestre), com acréscimo de novos requisitos como, por exemplo, de testes específicos em aplicações. No entanto, o serviço é pago por uso, não havendo obrigatoriedade de execução.

8. Levantamento de soluções

1. Alternativas de Contratação

1.1. Nesta seção, a equipe de planejamento da contratação consegue vislumbrar as alternativas avaliadas para a contratação, considerando três aspectos relevantes: prazo contratual, forma de agrupamento das soluções e modelo de estabelecimento dos serviços. A análise a seguir discute vantagens e desvantagens de cada opção, de forma a fundamentar a escolha mais adequada ao contexto institucional da CVM.

2. Prazo de Contratação (12, 24 ou 36 meses)

2.1. A contratação por 12 meses oferece maior flexibilidade para revisões frequentes dos serviços e eventuais ajustes de rota em contratações com menor maturidade. No entanto, esse prazo reduzido gera ciclos repetitivos de planejamento, seleção, fiscalização e transição, elevando os custos administrativos e reduzindo a continuidade dos serviços. Além disso, os serviços em tela requerem um período de estabilização após eventual migração entre as contratadas, inadequado para o prazo padrão de 12 meses de contratação.

2.2. O prazo de 24 meses atenua parte desse esforço, mas ainda não permite maturação plena das capacidades de defesa cibernética, especialmente em serviços que dependem de evolução contínua, como monitoramento, resposta a incidentes e gestão de vulnerabilidades.

2.3. Por sua vez, o prazo de 36 meses proporciona maior previsibilidade orçamentária, favorece a continuidade operacional e reduz a necessidade de transições recorrentes, garantindo melhor amadurecimento dos processos e das capacidades técnicas entregues. Embora represente menor flexibilidade contratual, sua estabilidade operacional e eficiência administrativa superam essa desvantagem.

3. Agrupamento das Soluções (itens separados, agrupamento parcial ou grupo único)

3.1. A contratação por itens separados maximiza a liberdade de escolha, mas aumenta a complexidade de integração entre ferramentas, gera potenciais incompatibilidades e fragmenta a responsabilidade técnica entre diversos fornecedores. Esse modelo pode comprometer a coerência da operação de segurança, que depende de correlação integrada de eventos e de agilidade de resposta.

3.2. O agrupamento total em um único lote reduz a fragmentação, simplifica a gestão e concentra a responsabilidade técnica, mas tende a restringir a competitividade e limitar o uso de soluções mais aderentes a demandas específicas. Adicionalmente, alguns serviços, como o do teste de invasão, visam justamente avaliar o adequado tratamento de vulnerabilidades e o monitoramento de eventos de segurança entregues pelos demais serviços.

3.3. O agrupamento parcial representa uma alternativa equilibrada: permite combinar especialidades distintas, reduz a fragmentação excessiva e preserva a competitividade entre fornecedores, ao mesmo tempo em que diminui riscos de incompatibilidade e facilita a coordenação da operação. Sua principal exigência é o cuidado na definição dos limites entre os grupos, o que é plenamente administrável diante dos benefícios.

4. Forma de Estabelecimento dos Serviços (ferramentas abertas, licenças próprias ou ferramentas + serviços contratados)

4.1. O uso exclusivo de ferramentas de código aberto possui custo de aquisição reduzido, porém demanda equipe interna altamente especializada e focada quase que exclusivamente nos aspectos técnicos do ambiente, longe, portanto, da realidade que se impõe na Administração Pública, além de maior esforço de manutenção, integração e

resposta. Em ambientes com capacidade operacional limitada, como é o caso da CVM, esse modelo compromete a efetividade da segurança e eleva riscos técnicos.

4.2. A aquisição de licenças de software com administração interna reduz parte da complexidade técnica das soluções, uma vez que parte da sustentação das soluções é terceirizada, mas mantém a necessidade de equipe própria para operação, análise de eventos, correlação de alertas, tratativas de vulnerabilidades e resposta a incidentes. Esse modelo exige escala e disponibilidade que não estão presentes na estrutura interna da autarquia.

4.3. A contratação de ferramentas acompanhadas de serviços especializados, por sua vez, assegura operação contínua, equipe dedicada, expertise atualizada, manutenção permanente e maior velocidade no tratamento de incidentes e de vulnerabilidades, além de ter sido validada ao longo dos últimos 5 anos de prestação dos serviços de MSS. Embora apresente custo financeiro superior, esse modelo reduz riscos operacionais, aumenta a eficiência da operação e permite que a área interna da CVM se concentre nas atividades estratégicas de supervisão e de governança.

9. Análise comparativa de soluções

1. Resumo das opções

1.1. Dentre as possibilidades apresentadas na seção 8 anterior, o quadro abaixo apresenta os quadro-resumo das alternativas, comparando-as entre si e excluindo aquelas que a equipe de planejamento entende como inviáveis.

1.2. Aspecto de prazo de contratação

Alternativa	Vantagens	Desvantagens	Considerar na análise?	Justificativa
12 meses	Flexibilidade; Permite revisões frequentes; prazo curto para a diluição de custos de implantação	Elevada carga administrativa; alto risco de rotatividade contratual; prazo reduzido para estabilização dos serviços	Não	Não garante continuidade nem estabilidade necessárias à evolução das capacidades de segurança.
24 meses	Menos ciclos de contratação; relativa continuidade;	Maturidade ainda limitada; janela de implementação mais curta que o ideal	Sim	Avaliação útil, mas insuficiente para suportar serviços complexos e contínuos de SI.
36 meses	Maior continuidade; diluição de custos; aumento da maturidade do serviço; previsibilidade operacional	Menor flexibilidade para correção de rota	Sim	Melhor relação entre estabilidade, maturidade, eficiência administrativa e qualidade da operação de segurança

1.3. Aspecto de agrupamento de itens

Alternativa	Vantagens	Desvantagens	Considerar na análise?	Justificativa
Itens separados	Maior liberdade de escolha; ampla competição	Fragmentação; incompatibilidades; múltiplos fornecedores; gestão complexa	Não	Aumenta riscos operacionais e dificulta integração essencial para correlação de eventos.
Agrupamento parcial	Reduz fragmentação; mantém competitividade; facilita coordenação; combina especialidades	Requer definição precisa dos limites entre grupos	Sim	Equilibra especialização, competitividade e coerência técnica, reduzindo riscos e complexidade.
Grupo único (indivisível)	Gestão simplificada; uma única responsabilidade técnica	Reduz competição; pode limitar a escolha de soluções mais adequadas	Não	Simplifica gestão, mas pode restringir competitividade e flexibilidade técnica.

1.4. Aspecto de forma de estabelecimento dos serviços

Alternativa	Vantagens	Desvantagens	Considerar na análise?	Justificativa
Ferramentas abertas (open source)	Baixo custo de aquisição; independência de fornecedor	Alta dependência de equipe interna; manutenção complexa; risco operacional elevado	Não	Incompatível com a capacidade operacional atual e com a criticidade dos serviços.
Licenças + administração interna	Reduz parte da complexidade; controle interno maior	Exige equipe dedicada; resposta mais lenta; risco de sobrecarga operacional	Não	Possível, mas pouco eficiente diante da estrutura reduzida e das demandas contínuas de SI.
Ferramentas + serviços especializados	Operação contínua 24x7; equipe dedicada; maior velocidade de resposta; menor risco operacional	Maior custo financeiro	Sim	Entrega o melhor equilíbrio entre eficácia, segurança, disponibilidade e capacidade técnica.

2. Alternativas viáveis para análise

Diante das considerações apresentadas nas tabelas acima, a equipe de planejamento da contratação fará uma análise pormenorizada dos prazos de **24 (vinte e quatro) e 36 (trinta e seis) meses**, que influenciam a disponibilidade de recursos financeiros para a execução dos serviços, mas considerará apenas as alternativas de **agrupamento parcial** dos itens listados, visando fomentar a competitividade saudável entre participantes do mercado sem aumentar significativamente o risco de execução para a CVM e a **contratação do conjunto ferramentas e serviços especializados**, dada a necessidade de monitoramento de segurança em regime 24 x 7 e a realidade da equipe técnica disponível na CVM.

10. Registro de soluções consideradas inviáveis

1. As opções que envolvem **prazo máximo de apenas 12 meses** foram descartadas porque não oferecem estabilidade nem previsibilidade para a execução do serviço. Um prazo tão curto aumenta o risco de interrupções, renovações emergenciais e perda de continuidade operacional — tudo aquilo que uma área crítica, como Segurança da Informação, não pode enfrentar.

2. A possibilidade de **desagrupar totalmente os serviços** também não será avaliada, pois fragmentar a contratação em partes isoladas dificulta o controle, aumenta a chance de falhas de coordenação entre fornecedores, eleva o esforço interno de gestão e aumenta a possibilidade de mais divergências e o risco de que a responsabilidade pelo problema “caia entre as cadeiras”.

3. Da mesma forma, a alternativa de **contratar tudo em um único bloco**, com um único fornecedor dominando todas as frentes, foi descartada. Embora pareça mais simples à primeira vista, ela reduz a flexibilidade, encarece ajustes futuros e pode gerar dependência excessiva de um único prestador — algo indesejável em serviços que precisam ser continuamente atualizados e auditáveis.

4. Por fim, optou-se por não seguir com o uso de **softwares abertos administrados internamente ou combinação de licenças + gestão própria**. Apesar de funcionarem bem em cenários menores, essas abordagens exigem equipe técnica especializada, dedicação constante, atualizações contínuas e uma estrutura interna que hoje não corresponde ao nível de maturidade necessário. Em outras palavras: a solução até poderia ser mais barata no papel, mas sairia mais cara em esforço, risco e exposição.

11. Análise comparativa de custos (TCO)

Para fins dessa análise comparativa de custos, a equipe técnica de contratação considerou exclusivamente o cenário 4, pois é o único cenário viável. O racional da pesquisa de preços está apresentado no Anexo ETP.III - Nota Técnica de Pesquisa de Preços DCIS/STI nº 001/2026.

12. Descrição da solução de TIC a ser contratada

1. A solução a ser contratada consiste em um **conjunto integrado de ferramentas especializadas e serviços técnicos profissionais** voltados ao fortalecimento da Segurança da Informação (SI) no ambiente da CVM. Esse conjunto deverá contemplar capacidades de identificação, avaliação e monitoramento contínuo de vulnerabilidades, detecção de ameaças, correlação de eventos, tratamento de incidentes e apoio à aplicação das políticas corporativas de segurança. As ferramentas devem operar de forma coordenada, garantindo visão abrangente do ecossistema tecnológico da autarquia e permitindo respostas tempestivas a riscos e a desvios.

2. Além dos recursos tecnológicos, a solução incluirá **serviços de suporte operacional, consultoria especializada e acompanhamento técnico**, assegurando o funcionamento adequado das plataformas, a interpretação dos dados coletados e a execução de ações necessárias ao saneamento das fragilidades identificadas. Esses serviços deverão abranger a configuração, operação assistida, análise contínua de segurança, produção de relatórios técnicos, orientação para mitigação de riscos e apoio direto no tratamento de incidentes, garantindo coerência com as normas e diretrizes vigentes na CVM.

3. A solução contratada deverá ainda apoiar ações de **governança e conscientização em SI**, provendo subsídios técnicos para a tomada de decisão, evidências para auditorias e insumos para atividades internas de sensibilização de usuários. O objetivo final é fortalecer a postura de segurança da autarquia, ampliando sua capacidade de prevenção, detecção e resposta, com ferramentas modernas e equipe especializada, dentro de um modelo sustentável e aderente às melhores práticas do setor.

4. Esta equipe de contratação atesta que os serviços a serem contratados se enquadram como atividades materiais acessórias, instrumentais ou complementares aos assuntos que constituem área de competência legal do órgão ou da entidade, conforme versa o Art. 48 da Lei 14133/21.

5. Vale atentar que os serviços objetos dessa contratação **não fazem parte do catálogo eletrônico de padronização** [1] **nem no Catálogo de Soluções de TIC com Condições Padronizadas**[2], disponíveis nos portais de Governo.

6. A Equipe de Planejamento da Contratação atesta, também, que o objeto desta contratação – Serviços Gerenciados de Segurança da Informação (MSS) – **não se insere no modelo de contratação disciplinado pela Portaria SGD /MGI nº 1.070, de 1º de junho de 2023**[3]**.** A presente demanda possui natureza estritamente voltada à segurança cibernética (contemplando serviços como monitoramento proativo, resposta a incidentes, gestão de vulnerabilidades e testes de invasão), escopo distinto das atividades de suporte técnico a usuários de TI (Service Desk) e da operação convencional de infraestrutura tecnológica (NOC) previstas na referida norma. Desta forma, certifica-se o não enquadramento legal e a não obrigatoriedade do modelo padronizado em questão.

7. A Equipe de Planejamento certifica, ainda, que a presente solução de Serviços Gerenciados de Segurança (MSS) **não se enquadra de forma estrita no modelo de contratação de software e de serviços de computação em nuvem previsto pela Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023**. Embora a contratada possa fornecer e se utilizar de plataformas de software e eventuais recursos em nuvem para viabilizar as entregas, o núcleo preponderante e indissociável da contratação é o provimento do esforço técnico humano – especializado e analítico –, consubstanciado na atuação de um Centro de Operações de Segurança (SOC) operando em 24/7. Trata-se, portanto, de contrato de prestação de serviços continuados sob demanda (apoio ao tratamento de incidentes, pentest etc.), em que as ferramentas tecnológicas configuram apenas o meio para execução do objeto, destoando da natureza de mera aquisição ou subscrição isolada de software/nuvem que pauta a referida Portaria.

8. Adicionalmente, a equipe de planejamento da contratação declara que os serviços pretendidos não incidem nas vedações dos artigos 3º e 4º da IN SGD nº 94/2022, considerando que: (i) constituem uma única solução de TIC; (ii) não envolvem gestão de processos de TIC nem gestão de segurança da informação; e (iii) não abrangem atividades de avaliação, mensuração ou apoio à fiscalização de contratos de TIC.

9. É importante ressaltar que a não utilização do Sistema de Registro de Preços (SRP) para a presente contratação justifica-se por se tratar de uma aquisição pontual de equipamentos e/ou serviços com quantitativos claramente

definidos, destinados exclusivamente a este órgão e sem previsão de demandas futuras recorrentes ou entregas parceladas, o que não se alinha às condições estabelecidas no Art. 3º do Decreto nº 11.462/2023.

10. Além disso, não se enquadra nas exceções do Art. 4º, uma vez que há histórico de demandas, o objeto não é perecível e o serviço não está indissociavelmente integrado ao fornecimento de bens, tornando a licitação convencional o método mais adequado e eficiente para atender à necessidade específica da Administração.

11. Por fim, a adesão a atas de registro de preços disponíveis dificilmente é viável para esse tipo de produto, uma vez que há relevante variabilidade entre as especificações técnicas das soluções existentes, o que restringe a participação da CVM em relação aos requisitos disponíveis. Soma-se a isso a possível incompatibilidade entre os prazos operados pelos órgãos gerenciadores e o cronograma exigido para a contratação na autarquia, o que traria riscos de descontinuidade. Diante desses fatores, a adesão não assegura as condições mínimas necessárias para a contratação pretendida.

[1] Disponível em https://www.gov.br/pncp/pt-br/catalogo-eletronico-de-padronizacao

[2]Disponível em https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/catalogos-de-solucoes-de-tic-com-condicoes-padronizadas-para-licenciamento-de-software

[3]Disponível em https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/legislacao/modelo-de-contracao-de-servicos-de-operacao-de-infraestrutura-e-de-atendimento-a-usuarios-de-tic/portaria-sgd-mgi-no-1-070-de-1o-de-junho-de-2023

[4]Disponível em https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/vigentes/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023

13. Estimativa de custo total da contratação

Valor (R$): 7.136.915,43

13.1. A estimativa de custo unitário e total por subitem segue de acordo com a tabela abaixo:

Grupo	Item	Descrição	Subitem	Serviço	CATSER	Métrica	Volume Máximo	Custo unitário	Custo Total (36 meses)
1	1	Gestão de Vulnerabilidades	1.1	Licenças de software	27502	Unidade/mês	2000	R$ 30,10	R$ 2.167.200,00
			1.2	Serviço de administração	27014	Mês	36	R$ 13.349,17	R$ 480.570,12
			1.3	Treinamento	3840	Unidade	2	R$ 9.336,34	R$ 18.672,68
	2	Monitoramento e resposta a incidentes	2.1	Ferramentas de monitoramento	27502	Mês	36	R$ 23.662,74	R$ 851.858,64
			2.2	Serviço de administração	27014	Mês	36	R$ 39.196,10	R$ 1.411.059,60
			2.3	Treinamento	3840	Unidade	2	R$ 22.104,25	R$ 44.208,50
	3	Inteligência de ameaças cibernéticas	3.1	Serviço de administração	27014	Mês	36	R$ 24.026,07	R$ 864.938,52
			3.2	Takedowns	27014	Unidades	180	R$ 67,94	R$ 12.229,20
			3.3	Treinamento	3840	Unidade	2	R$ 9.096,06	R$ 18.192,12
2	4	Proteção de endpoints	4.1	Licenças de software	27502	Unidades/mês	1000	R$ 13,99	R$ 503.640,00
			4.2	Serviço de administração	27014	Mês	36	R$ 8.993,11	R$ 323.751,96
			4.3	Treinamento	3840	Unidade	2	R$ 23.002,01	R$ 46.004,02
3	5	Conscientização em segurança da informação	5.1	Licenças de uso	27502	Unidades/mês	800	R$ 7,07	R$ 203.616,00
			5.2	Serviço de implantação	26972	Pgto. Único	1	R$ 16.371,67	R$ 16.371,67
			5.3	Consultoria Técnica	27340	Horas	240	R$ 102,51	R$ 24.602,40
4	6	Testes de invasão	6.1	Execução de pentest	27014	Unidades	12	R$ 12.500,00	R$ 150.000,00

13.2. Os subitens da contratação possuem naturezas distintas de pagamento, relevantes para a composição do custo estimado e para a futura execução contratual:

13.2.1. **Subitens de pagamento recorrente mensal** (1.1, 1.2, 2.1, 2.2, 3.1, 4.1, 4.2 e 5.1): referem-se a licenças de software e serviços de administração cuja prestação é contínua, com pagamento mensal fixo vinculado à disponibilização do serviço;

13.2.2. **Subitens de pagamento sob demanda** (1.3, 2.3, 3.2, 3.3, 4.3, 5.3 e 6.1): compreendem treinamentos, takedowns, consultoria técnica e execução de testes de invasão, cujo pagamento ocorre por unidade efetivamente consumida, mediante ordem de serviço ou comprovação de execução; e

13.2.3. **Subitem de pagamento único** (5.2): refere-se ao serviço de implantação da solução de conscientização, com desembolso vinculado à entrega e ao aceite do serviço.

13.3. Contudo, a execução média mensal do contrato será iniciada com os volumes efetivamente dimensionados no **Anexo ETP.I - Especificação Técnica da Solução**, que são inferiores aos limites máximos.

13.4. Maiores detalhes do racional utilizado e a obtenção dos valores de referência podem ser obtidos no **Anexo ETP.III - Nota Técnica de Pesquisa de Preços.**

14. Justificativa técnica da escolha da solução

1. A adoção do **prazo de 36 meses** apresenta-se como a alternativa mais adequada para garantir continuidade operacional, estabilidade dos serviços e previsibilidade orçamentária. Um período mais longo reduz a ocorrência de interrupções típicas de renovações frequentes, viabiliza ciclos completos de implantação, maturação e melhoria contínua, além de permitir que o fornecedor entregue resultados evolutivos com maior segurança. Para a Administração, esse prazo reduz custos transacionais, minimiza riscos de descontinuidade e favorece o acompanhamento consistente de indicadores e metas.

2. O **agrupamento parcial das soluções** equilibra, de forma eficiente, a necessidade de coordenação centralizada com a flexibilidade para ajustes específicos. Ao concentrar os componentes que possuem forte interdependência técnica, evita-se fragmentação excessiva e sobrecarga de gestão. Ao mesmo tempo, o modelo não engessa a contratação em um bloco único, preservando competitividade, espaço para inovação e capacidade de substituir partes da solução caso surjam necessidades futuras. Trata-se de um arranjo que reduz riscos operacionais sem comprometer a adaptabilidade do ambiente.

3. A opção por **ferramentas acompanhadas de serviços especializados** assegura que a solução contratada opere com o nível de qualidade, atualização e resposta adequado ao contexto atual de segurança da informação. A combinação de tecnologia e equipe especializada permite que a Administração se beneficie de expertise contínua, melhores práticas consolidadas e configuração adequada das ferramentas ao longo de todo o contrato. Além disso, mitiga-se a dependência de equipes internas para atividades altamente técnicas, liberando capacidade institucional para focar na gestão e nos resultados estratégicos.

4. Por fim, essa composição — prazo estendido, agrupamento parcial e fornecimento integrado de ferramentas e serviços — forma um modelo de contratação equilibrado, sustentável e alinhado às necessidades de continuidade, segurança e eficiência operacional. O arranjo proposto reduz riscos, otimiza recursos e oferece o cenário mais favorável para alcançar os objetivos estabelecidos no planejamento.

15. Justificativa econômica da escolha da solução

Conforme descrito nas seções 8 a 14 deste Estudo Técnico Preliminar.

16. Benefícios a serem alcançados com a contratação

1. A contratação deve permitir identificar, avaliar e monitorar vulnerabilidades de segurança de forma contínua, fortalecendo o tratamento de riscos e elevando o nível de proteção dos ambientes tecnológicos atualmente expostos.

2. O serviço deverá proporcionar capacidade estruturada para acompanhar o surgimento e a propagação de ataques cibernéticos, possibilitando a identificação preventiva de ameaças que possam representar riscos à CVM.

3. A solução contratada visa ampliar a capacidade de resposta a incidentes de Segurança da Informação, permitindo restauração rápida dos ambientes afetados, identificação precisa das vulnerabilidades exploradas e sua correção sempre que tecnicamente viável.

4. A execução das políticas e regras de segurança definidas pela equipe técnica precisa ser fortalecida, assegurando o uso adequado do parque tecnológico, reduzindo acessos indevidos e mitigando o risco de vazamento de informações sensíveis.

5. As ações de conscientização dos usuários ganharão escala e continuidade, difundindo boas práticas de segurança e contribuindo para a redução de vulnerabilidades decorrentes de comportamento humano.

6. A contratação também trará maior agilidade no tratamento das demandas de Segurança da Informação, garantindo respostas mais tempestivas e alinhadas às necessidades críticas da autarquia.

7. Por fim, os serviços contratados visam atender e manter atendidas medidas do Programa de Privacidade e Segurança da Informação - PPSI elencadas como prioritárias pela Secretaria de Governo Digital - SGD.

17. Providências a serem Adotadas

1. Considerando que a presente contratação tem por objeto a continuidade dos serviços de segurança atualmente prestados, com a eventual substituição dos equipamentos anteriormente utilizados, e levando em conta que o espaço físico e a infraestrutura elétrica já se encontram adequadamente dimensionados e preparados para esse tipo de operação, conclui-se que não há necessidade de adoção de novas providências. A contratação, portanto, dá-se em condições equivalentes às já existentes, sem implicar alterações estruturais ou operacionais no ambiente atual.

2. Adicionalmente, as ferramentas de software são majoritariamente fornecidas como serviço (SaaS), exigindo apenas a comunicação e acesso via Internet, não exigindo preparação adicional no ambiente da CVM.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

A Equipe de Planejamento da Contratação declara o presente estudo técnico preliminar viável do ponto de vista técnico, de negócio e econômico, desde que sejam adotadas as premissas e conclusões descritas neste documento conforme preconizado na IN. SGD/ME Nº 94/2022.

19. Responsáveis

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

Despacho: Integrante Técnico da Solução

RAFAEL MUNINHAS SERVO

Agente de contratação

Assinou eletronicamente em 16/06/2026 às 14:37:36.

Despacho: Integrante Técnico da Solução

MARLON CORDEIRO DOMENECH

Agente de contratação

Assinou eletronicamente em 16/06/2026 às 14:06:17.

Despacho: Integrante Requisitante da Solução

VINICIUS GAGNO LIMA

Agente de contratação

Assinou eletronicamente em 16/06/2026 às 13:47:58.

Despacho: Superintendente Interino

GUSTAVO HENRIQUE GORI MAIA

Autoridade competente

Assinou eletronicamente em 17/06/2026 às 15:30:15.