NOTA TÉCNICA STI/DCIS nº 002/2026

I - OBJETO DA CONTRATAÇÃO

1.1. O objeto da presente contratação visa o fornecimento de Serviços Gerenciados de Segurança (MSS - *Managed Security Services*), abrangendo, de forma integrada e contínua: serviço de gestão de vulnerabilidades, serviço de monitoramento e resposta a incidentes, serviço de inteligência de ameaças cibernéticas, serviço de proteção de *endpoints*, serviço de conscientização em segurança da informação e serviço de testes de invasão. A prestação continuada será mensurada por serviço, durante 36 (trinta e seis) meses, nos termos do Termo de Referência 139/2025, conforme condições e exigências estabelecidas neste instrumento.

1.2. A contratação visa manter e evoluir as soluções atualmente existentes no ambiente da CVM, cujo contrato atual se encerra em agosto/2026, garantindo assim a continuidade e evolução dos serviços listados acima, aumentando a visibilidade nas soluções adotadas pela autarquia e mantendo o atendimento de medidas elencadas como prioritárias no Programa de Privacidade e Segurança da Informação – PPSI.

II – OBJETIVO DO DOCUMENTO

2.1. Este documento visa apresentar os níveis mínimos de serviço (NMS) exigidos para a contratação dos serviços deste processo, em conformidade com as boas práticas e referências editalícias de outros órgãos da administração pública e demais diretrizes legais, cuja avaliação utilizará o Instrumento de Medição de Resultado (IMR). Para efeitos de desconto, todos os prazos contam a partir da data de implantação dos referidos serviços.

2.2. Para melhor entendimento, informamos que o Nível Mínimo de Serviços consiste no conjunto de indicadores, metas e mecanismos de controle destinados a assegurar que os serviços contratados sejam prestados com níveis adequados de qualidade, disponibilidade, desempenho e continuidade, permitindo a aferição objetiva dos resultados e a aplicação de ajustes financeiros ou sanções, quando cabível.

2.3. Os serviços contratados serão avaliados por meio de indicadores objetivos, mensuráveis e verificáveis, alinhados às boas práticas de gestão de contratos de TI, contemplando, no mínimo:

- Disponibilidade dos serviços;
- Tempo de atendimento de chamados;
- Tempo de solução de chamados;

- Conformidade técnica das entregas;
- Continuidade e estabilidade operacional;
- Qualidade do suporte técnico prestado.

III. CLASSIFICAÇÃO DE CRITICIDADE

3.1. Para fins de gestão do atendimento, resposta e solução das ocorrências observáveis relacionadas aos serviços contratados, as quais podem ser eventos, incidentes ou requisições, estas serão classificadas conforme seu nível de criticidade, considerando o impacto potencial ou efetivo sobre a confidencialidade, integridade e disponibilidade das informações, sistemas e serviços da CVM.

3.2. Serão classificados como **ocorrências emergenciais** aquelas que resultem em indisponibilidade total de sistemas críticos, envolvam ataques cibernéticos relevantes, infecção por *malware* ou *ransonware*, vazamento, exfiltração ou comprometimento de dados sensíveis, bem como quaisquer eventos que representem risco imediato e significativo à segurança da informação ou à continuidade das atividades institucionais

3.3. A classificação **alta** será atribuída às ocorrências que afetem sistemas de produção ou serviços relevantes, ocasionem degradação significativa de desempenho, envolvam alertas críticos identificados pelas ferramentas de segurança ou impactem usuários, processos ou ativos considerados críticos pela Administração.

3.4. As ocorrências classificadas como **médias** compreendem aquelas que não afetam sistemas críticos nem acarretam risco relevante de perda de dados, incluindo alertas que demandem análise técnica, correlação de eventos ou validação por parte da equipe especializada.

3.5. As ocorrências de **baixa criticidade** abrangem eventos de segurança legítimos, requisições, solicitações de informação, dúvidas operacionais, demandas de apoio técnico, mudanças planejadas, atividades de melhoria contínua, novas implementações previamente autorizadas e alertas de baixo impacto operacional ou de segurança.

IV. INDICADORES E NÍVEIS MÍNIMOS DE SERVIÇO

4.1. A execução dos serviços será avaliada mensalmente por meio de um conjunto consolidado de Indicadores de Nível Mínimo de Serviço (NMS), os quais abrangem aspectos operacionais, de qualidade da prestação e de gestão do serviço, permitindo a aferição objetiva do desempenho da contratada e a aplicação proporcional de descontos financeiros.

4.2. Os indicadores contemplam, entre outros aspectos, a disponibilidade dos serviços, os tempos máximos de triagem, resposta, correção e comunicação de incidentes, bem como a

tempestividade na entrega de relatórios e demais obrigações associadas à prestação dos serviços.

4.3. Os indicadores, respectivas fórmulas de cálculo, metas exigidas e critérios de desconto encontram-se detalhados na tabela a seguir, devendo ser observados durante toda a vigência contratual:

Tabela – Indicadores de Nível Mínimo de Serviço e Critérios de Glosa

Nº	Dimensão	Indicador	Descrição do Indicador	Fórmula de Cálculo	Meta	Glosa por inadimplemento
1	Operacional	Disponibilidade dos serviços	Mede o percentual de tempo em que os serviços contratados permaneceram disponíveis e operacionais no período de apuração	(Tempo disponível / Tempo total do período) × 100	≥ 99% para cada um dos itens 1.1, 2.1, 4.1 e 5.1	+5 pontos a cada 0,1% abaixo da meta
2	Operacional	Índice de Monitoramento da Infraestrutura (Ativos Comuns)	Mede o percentual de ativos comuns (estações de trabalho e equipamentos de IoT) cujos logs estão sendo enviados integralmente para o SIEM e corretamente processados	(total de ativos monitorados / total de ativos homologados pela CVM para serem monitorados) x 100	> 95% para o item 2.1	+5 pontos a cada 0,3% abaixo da meta
3	Operacional	Índice de Monitoramento da Infraestrutura (Ativos Relevantes)	Mede o percentual de ativos relevantes (servidores e serviços de qualquer natureza, proxies, switches de distribuição e acesso) cujos logs estão sendo enviados integralmente para o SIEM e corretamente processados	(total de ativos monitorados / total de ativos homologados pela CVM para serem monitorados) x 100	> 98% para o item 2.1	+15 pontos a cada 0,3% abaixo da meta
4	Operacional	Índice de Monitoramento da Infraestrutura (Ativos Críticos)	Mede o percentual de ativos críticos (firewalls, switches core, controladores de domínio, servidores e serviços de autenticação - RADIUS, LDAP, SAML etc. - e serviços DNS) cujos logs estão sendo enviados integralmente para o SIEM e corretamente processados	(total de ativos monitorados / total de ativos homologados pela CVM para serem monitorados) x 100	100% para o item 2.1	+15 pontos a cada 1% abaixo da meta
5	Operacional	Tempo de correção de incidente com indisponibilidade	Mede o tempo decorrido entre a identificação do incidente e o completo restabelecimento do serviço afetado	Hora do restabelecimento − Hora do início	≤ 60 minutos para cada um dos itens 1.1, 2.1, 4.1 e 5.1	+5 pontos a cada 10 minutos excedentes
6	Operacional	Tempo de correção de incidente com degradação de desempenho	Mede o tempo para solução de incidentes que causem degradação relevante, sem indisponibilidade total	Hora do restabelecimento − Hora do início	≤ 120 minutos para cada um dos itens 1.1, 2.1, 4.1 e 5.1	+5 pontos a cada 10 minutos excedentes
7	Operacional	Tempo de triagem de incidentes	Mede o tempo entre a abertura do chamado e sua correta classificação quanto à criticidade	Hora da triagem − Hora de abertura	≤ 15 minutos para os itens 1.2, 2.2, 3.1 e 4.2	+1 ponto a cada 5 minutos excedentes

8	Operacional	Tempo de resposta a ocorrências emergenciais	Mede o tempo entre a triagem e o início efetivo do atendimento técnico	Hora do início da resposta − Hora da triagem	≤ 30 minutos para os itens 1.2, 2.2, 3.1 e 4.2	+5 pontos a cada 5 minutos excedentes
9	Operacional	Tempo de resposta a ocorrências de alta criticidade	Mede o tempo entre a triagem e o início efetivo do atendimento técnico	Hora do início da resposta − Hora da triagem	≤ 60 minutos para os itens 1.2, 2.2, 3.1 e 4.2	+4 pontos a cada 5 minutos excedentes
10	Operacional	Tempo de resposta a ocorrências de média e baixa criticidade	Mede o tempo entre a triagem e o início efetivo do atendimento técnico	Hora do início da resposta − Hora da triagem	≤ 240 minutos para os itens 1.2, 2.2, 3.1 e 4.2	+3 pontos a cada 5 minutos excedentes
11	Governança	Comunicação de ocorrências de criticidade emergencial e alta	Mede a tempestividade da comunicação formal à Administração sobre ocorrências relevantes	Hora da comunicação − Hora da triagem	≤ 15 minutos, para os itens 1, 2, 3, 4 e 5	+2 pontos a cada 5 minutos excedentes
12	Governança	Entrega de relatório mensal	Mede o cumprimento do prazo para entrega do relatório consolidado de atendimentos e indicadores	Data de entrega − Data limite	Até o 3º dia útil do mês subsequente, para os itens 1, 2, 3, 4 e 5	+2 pontos a cada 24 horas de atraso
13	Governança	Cumprimento de planos de ação e prazos acordados	Deixar de cumprir prazos definidos em ata de reunião	Identificação de ocorrência por parte da CVM	0 ocorrências, para cada item	15 pontos por ocorrência
14	Governança	Falta de qualificação profissional	Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, ainda que em casos de substituição temporária.	Identificação de ocorrência por parte da CVM	0 ocorrências, para cada item	15 pontos por ocorrência
15	Governança	Manipulação de indicador	Fraudar, manipular ou descaracterizar indicadores/metas de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado.	Identificação de ocorrência por parte da CVM	0 ocorrências, para cada grupo	30 pontos por ocorrência
16	Governança	Não indicar preposto	Deixar de indicar preposto ou deixá-la desatualizada para acompanhamento da execução contratual	Identificação de ocorrência por parte da CVM	0 ocorrências, para cada grupo	20 pontos por ocorrência
17	Qualidade	Falha no atingimento do NMS consecutivo	Não atingir nível mínimo de serviço, apurados em um período de 12 meses	3 meses consecutivos	0 ocorrências, para cada item	30 pontos por ocorrência

18	Qualidade	Falha no atingimento do NMS alternado	Não atingir nível mínimo de serviço, apurados em um período de 12 meses	5 meses alternados	0 ocorrências, para cada item	60 pontos por ocorrência
19	Qualidade	Controle de mudanças	Realizar mudanças de configuração nas soluções de segurança sem autorização da equipe CVM	Por regra, política ou baseline incluída, alterada ou excluída sem solicitação formal	0 ocorrências para os itens 1.2, 2.2, 3.1 e 4.2	15 pontos por ocorrência
20	Qualidade	Falha na ingestão de logs	Mede a divergência entre os logs recebidos pela ferramenta de monitoramento da CONTRATADA e os logs recebidos por ferramenta gerenciada pela CVM	Por ativo, regra ou arquivo de log monitorado	< 5%, para o item 2.1	5 pontos por ocorrência
21	Qualidade	Falha na retenção de logs	Mede a quantidade de ocorrências identificadas de falha de retenção de logs por, pelo menos, 1 (um) ano	Por ocorrência	0 ocorrências, para o item 2.1	5 pontos por ocorrência

V – FORMA DE MEDIÇÃO E APURAÇÃO DOS RESULTADOS

5.1. A apuração dos níveis mínimos de serviço será realizada mensalmente, por meio do Instrumento de Medição de Resultado (IMR), com base em informações extraídas das ferramentas de monitoramento, sistemas de gestão de chamados, relatórios técnicos, registros de auditoria e demais evidências necessárias à comprovação da execução dos serviços.

5.2. Caberá à fiscalização do contrato analisar, validar e homologar os resultados apresentados, podendo solicitar esclarecimentos, ajustes ou evidências adicionais sempre que julgar necessário para a correta aferição do desempenho da contratada.

5.3. Para fins de contagem de prazos e aplicação de descontos, considerar-se-á como marco inicial a data de implantação efetiva de cada serviço, conforme cronograma aprovado pela CVM.

VI – APLICAÇÃO DE DESCONTOS E GLOSAS

6.1. O não atingimento das metas estabelecidas para os indicadores de nível mínimo de serviço acarretará a apuração de pontuação negativa, a qual será convertida em desconto financeiro, nos termos definidos neste Anexo.

6.2. A conversão da pontuação em glosa observará o critério de 1% (um por cento) de desconto para cada 15 (quinze) pontos, limitada a 20% (vinte por cento) do valor mensal contratado, referente ao serviço impactado, conforme apresentado na coluna “Meta” da Tabela – Indicadores de Nível Mínimo de Serviço e Critérios de Glosa deste Anexo, resguardado o contraditório e a ampla defesa da contratada.

6.3. Caso o montante de desconto apurado ultrapasse o limite mensal estabelecido, o saldo excedente poderá ser compensado nas faturas subsequentes, excetuado o último mês de vigência contratual.

VII – DISPOSIÇÕES FINAIS

7.1. A aplicação dos níveis mínimos de serviço e dos respectivos descontos não exclui a adoção de outros mecanismos de fiscalização, controle e responsabilização previstos no contrato, no Termo de Referência e na legislação aplicável.

7.2. O descumprimento reiterado dos níveis mínimos de serviço poderá caracterizar inexecução parcial ou total do contrato, ensejando a aplicação das sanções administrativas cabíveis.

7.3. Os indicadores e níveis mínimos de serviço poderão ser revistos, desde que devidamente justificados sob o aspecto técnico e formalizados mediante instrumento próprio, com aprovação da Administração.