EDITAL DE PREGÃO BDMG-19/2026

Processo SEI: 5200.01.0001451/2026-91
Modalidade: **PREGÃO ELETRÔNICO**
Tipo: **MENOR PREÇO**
Adjudicação por **MENOR VALOR GLOBAL**
PROCESSO DE COMPRAS NO PORTAL COMPRAS MG: **5201006 000006/2026**
Unidade de compra – **5201006**
Nº do processo de compra – **000006**
Ano do processo de compra – **2026**

OBJETO: Contratação de empresa especializada na prestação de serviços gerenciados de Centro de Operações de Segurança (SOC), em regime de operação contínua 24x7x365, conforme as especificações descritas e detalhadas neste edital e em seus anexos**.**

ANEXOS:
ANEXO I – TERMO DE REFERÊNCIA
ANEXO II – CONDIÇÕES E DOCUMENTOS DE HABILITAÇÃO
ANEXO III – CONDIÇÕES E FORMA DE APRESENTAÇÃO DAS PROPOSTAS COMERCIAIS
ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL

ATENÇÃO: textos destacados em azul contêm links para seções deste documento, páginas da internet, ou arquivos.

ABERTURA DO CERTAME: a sessão pública será realizada em ambiente virtual, na rede mundial de computadores – internet, no Portal de Compras – MG, pelo endereço eletrônico www.compras.mg.gov.br.

DATA: 25/11/2026.
HORA: 09h30 no horário de Brasília/DF.

CONSULTA AO EDITAL E DIVULGAÇÃO DE INFORMAÇÕES:
https://www.bdmg.mg.gov.br/editais-licitacoes/ ou http://www.compras.mg.gov.br

ESCLARECIMENTOS E IMPUGNAÇÕES – na forma do item 2.3

Os interessados deverão consultar diariamente as páginas referentes a esta licitação, no portal do BDMG e no Portal de Compras - MG, nas quais serão publicados avisos, eventuais alterações e versões digitalizadas de documentos produzidos no âmbito do certame.

SUMÁRIO

1. PREÂMBULO.....4

2. DAS ALTERAÇÕES, DAS CONSULTAS E ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL.....4

3. DAS CONDIÇÕES DE PARTICIPAÇÃO.....5

3.3. Estão impedidos de participar:..... 5

3.6. Das regras gerais para apresentação de documentação..... 6

3.7. Do cadastramento para acesso ao sistema de pregão eletrônico 7

3.8. Da proposta comercial..... 8

3.9. Da documentação para habilitação 9

3.9.2. Utilização do Certificado de Registro Cadastral - CRC..... 9

3.9.3. Da restrição na documentação de microempresas, empresas de pequeno porte e equiparados 10

4. DAS REGRAS GERAIS DO PREGÃO 10

4.6. Da contagem de prazos 10

4.7. Das prerrogativas do Pregoeiro..... 10

5. DA SESSÃO PÚBLICA 11

5.1. Abertura da sessão pública 11

5.2. Suspensão da sessão pública..... 12

6. DOS PROCEDIMENTOS PARA SELEÇÃO DA MELHOR PROPOSTA..... 12

6.1. Da fase de lances 12

6.2. Do privilégio às ME, EPP ou equiparadas (empate ficto) 14

6.3. Da verificação da conformidade da proposta..... 14

6.4. Da análise quanto à exequibilidade 15

6.5. Da negociação com o então mais bem classificado..... 15

6.6. Da análise da documentação de habilitação 16

6.7. Da apresentação de documentação suplementar por ME, EPP ou equiparada..... 17

6.8. Da possibilidade de apresentação de nova documentação..... 17

6.9. Da classificação final e adjudicação do objeto 17

6.10. Orientações para participação da sessão pública 18

7. DOS RECURSOS 18

8. DA HOMOLOGAÇÃO 20

9. DA ASSINATURA DO INSTRUMENTO CONTRATUAL..... 20

9.2.1. Sobre o instrumento contratual em vias digitais assinadas mediante plataforma de assinaturas eletrônicas 20

9.2.2. Sobre o instrumento contratual em vias que são documentos natos SEI-MG assinados mediante procedimentos próprios desse sistema 20

9.2.3. Sobre o instrumento contratual em vias impressas em papel 21

10. DAS PENALIDADES 22

11. DISPOSIÇÕES GERAIS 23

12. FORO 23

ANEXO I – TERMO DE REFERÊNCIA 24

ANEXO II – CONDIÇÕES E DOCUMENTOS DE HABILITAÇÃO 28

ANEXO III – CONDIÇÕES E FORMA DE APRESENTAÇÃO DAS PROPOSTAS COMERCIAIS 33

ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL 38

ANEXO IV-A – TERMO DE REFERÊNCIA – REQUISITOS 63

1. PREÂMBULO

O **BANCO DE DESENVOLVIMENTO DE MINAS GERAIS S.A. – BDMG**, empresa pública com sede na Rua da Bahia, 1.600, Belo Horizonte, MG, CNPJ nº 38.486.817/0001-94, a seguir denominado simplesmente BDMG, torna pública a realização da licitação indicada na folha de rosto deste Edital. A presente licitação, devidamente autorizada por autoridade competente consoante normas internas, reger-se-á pelos seguintes normativos ou por outros que os substituírem: Lei Federal nº 13.303/2016; Lei Federal 14.133/2021, apenas em relação ao rito procedimental do pregão na fase externa da licitação, enquanto diretriz; Lei Estadual nº 13.994/2001; Decreto Estadual nº 45.902/2012; Decreto Estadual nº 47.154/2017; Decreto Estadual 48.723/2023, apenas em relação ao rito procedimental do pregão na fase externa da licitação, enquanto diretriz; o Regulamento de Licitações e Contratos do BDMG e legislação supletiva, bem como pelas normas, procedimentos e cláusulas deste Edital e dos seus anexos, os quais o integram para todos os efeitos legais.

2. DAS ALTERAÇÕES, DAS CONSULTAS E ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

2.1. O Edital completo encontra-se disponível no portal do **BDMG** na internet, no endereço https://www.bdmg.mg.gov.br/editais-licitacoes, e no Portal de Compras – MG, no endereço http://www.compras.mg.gov.br.

2.2. Os interessados deverão consultar diariamente a página referente a esta licitação no portal do **BDMG** e no Portal de Compras - MG, nos quais serão publicados avisos, eventuais alterações e versões digitalizadas de documentos produzidos no âmbito do certame.

2.2.1. As modificações promovidas no instrumento convocatório serão objeto de divulgação nos mesmos termos e prazos dos atos e procedimentos originais, exceto quando a alteração não afetar a preparação das propostas, caso em que, no portal Compras MG, será publicada mediante a funcionalidade 'quadro de avisos'.

2.2.1.1. ATENÇÃO: cabe ao licitante a diligência de verificar a necessidade de recadastramento de sua proposta original, a qual será suprimida pelo sistema, a depender do teor da alteração empreendida no edital.

2.3. Serão conhecidos os pedidos de esclarecimentos e impugnações ao Edital que forem apresentados até o dia 18/11/2026, mediante o preenchimento do formulário eletrônico próprio no Portal de Compras MG, com informação dos seguintes dados:

I – se pessoa física, nome, CPF, data de nascimento e e-mail.

II – se pessoa jurídica, nome, CNPJ, nome do representante, data de nascimento do representante, comprovação dos poderes de representação do representante e e-mail.

2.3.1. A comprovação dos poderes de representação a que se refere o item 2.3, inciso II, supra será mediante o encaminhamento da documentação pertinente, por upload, quando do preenchimento do formulário eletrônico relativo ao pedido de esclarecimento ou impugnação.

2.3.2. A informação da data de nascimento do demandante ou do representante do demandante será feita no campo 'Mensagem' do formulário eletrônico, com o pedido de esclarecimento ou impugnação.

2.3.3. Um tutorial com orientações de como encaminhar os pedidos de esclarecimentos e impugnações pode ser acessado pelo link incluído AQUI, **observadas as condições dos itens 2.3 a 2.3.2, supra.**

2.3.4. Não serão conhecidos os pedidos de esclarecimento e impugnações sem informação dos dados de identificação e juntada da documentação referidos no item 2.3, incisos I e II.

2.3.5. As informações a que se refere o item 2.3, incisos I e II, serão obtidas mediante consulta ao respectivo CRC do interessado, no CAGEF-MG, se houver e conforme o caso.

2.4. O Pregoeiro julgará e responderá à impugnação e/ou pedido de esclarecimento no prazo de 03 (três) dias úteis contados do seu recebimento pelo **BDMG**.

3. DAS CONDIÇÕES DE PARTICIPAÇÃO

3.1. A participação no pregão eletrônico se dará por meio da digitação da senha privativa da licitante e do subsequente encaminhamento de proposta de preço até a data e horário previstos no edital.

3.2. Podem participar do certame aqueles que atuem no ramo pertinente ao objeto licitado, observadas as exigências dispostas neste Edital.

3.3. Estão impedidos de participar:

I – pessoa jurídica com falência declarada, em dissolução ou liquidação;

II – pessoa jurídica que contenha no seu contrato ou estatuto social finalidade ou objetivo incompatível com o objeto desta licitação;

III – pessoa jurídica cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social e seja dirigente ou empregado do **BDMG**;

IV – pessoa jurídica que esteja cumprindo a pena de suspensão do direito de licitar e contratar aplicada pelo **BDMG**;

V – pessoa jurídica incluída no Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS previsto na Lei Federal nº 12.846/2013 ou no Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual – CAFIMP previsto na Lei Estadual nº 13.994/2001;

VI – pessoa jurídica constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;

VII – pessoa jurídica cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea;

VIII – pessoa jurídica constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

IX – pessoa jurídica cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

X – pessoa jurídica que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea;

XI – empregado ou dirigente do **BDMG**;

XII – pessoa física que tenha relação de parentesco, até o terceiro grau civil, com:

a) dirigente do **BDMG**;

b) empregado do **BDMG** cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

c) autoridade do Estado de Minas Gerais, assim entendido aqueles que exercem o cargo de Secretários de Estado, Diretores Gerais, Presidentes de Estatais e de Órgãos da Administração Direta, Indireta, Autárquica, Fundacional.

XIII – pessoa jurídica cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com o **BDMG** ou do **BDMG** há menos de 6 (seis) meses.

XIV – pessoas jurídicas organizadas sob a forma de consórcio.

XV – duas ou mais sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum;

XVI – pessoa jurídica estrangeira que não tenha representação legal no País ou que esta representação legal não tenha poderes expressos para receber citação e responder administrativa ou judicialmente;

XVII – pessoa física não equiparada a jurídica.

3.4. As licitantes assumirão todos os custos devidos para a participação nesta licitação, não sendo o **BDMG** em nenhum caso responsável por tais ônus, independentemente da condução ou do resultado do processo licitatório.

3.5. Não poderá se beneficiar do tratamento jurídico diferenciado previsto na Lei Complementar Federal 123/2006 licitante que incida em qualquer das hipóteses previstas no art. 3º, §4º, desta mesma lei.

3.6. Das regras gerais para apresentação de documentação

3.6.1. As licitantes serão responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

3.6.1.1. A constatação de que qualquer dos documentos apresentados não corresponde à realidade implicará na imediata inabilitação ou desclassificação da licitante, sem prejuízo das demais sanções cabíveis.

3.6.2. Os documentos apresentados para esta licitação se referirão a uma única pessoa jurídica, não sendo admitida a apresentação de uma parte dos documentos em nome de matriz e outra em nome de filial ou em nome de filiais diferentes, exceto em relação à documentação emitida exclusivamente em nome da matriz, sob pena de imediata inabilitação no certame.

3.6.2.1. No caso da habilitação técnica, serão aceitos atestados emitidos em nome da matriz ou da filial.

3.6.3. Os documentos apresentados deverão ser válidos e vigentes na data da abertura da sessão pública.

3.6.3.1. Os documentos que perderem validade e/ou vigência no curso da licitação serão reapresentados válidos e vigentes na data da assinatura do Instrumento Contratual.

3.6.4. Cada documento apresentado em via física no âmbito da licitação, exceto no caso de certidão disponível na internet, será em via original, cópia autenticada em cartório ou cópia não autenticada acompanhada do respectivo original.

3.6.5. O documento cuja validade, vigência e/ou autenticidade seja aferível pela *internet* será verificado pelo Pregoeiro no sítio eletrônico pertinente.

3.6.5.1. Serão aceitos documentos em vias digitais assinadas mediante certificação digital, desde que comprovada pelo Pregoeiro a autenticidade da firma eletrônica.

3.6.6. Os documentos expressos em língua estrangeira serão inicialmente apresentados em tradução livre, devendo ser apresentados, como condição prévia de contratação, traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto Federal nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas, caso o licitante que os apresenta venha a ser declarado vencedor da licitação.

3.6.7. Não serão aceitos protocolos de entrega ou solicitação de documentos em substituição aos documentos requeridos neste Edital.

3.6.8. A licitante que estiver desobrigada de apresentar quaisquer documentos ou informação exigidos no certame ou exigidos para a execução contratual deverá comprovar tal condição por meio de certificado expedido pelo órgão competente ou pela indicação da legislação aplicável em vigor, devendo, no entanto, apresentar os documentos que a sua condição indicar como substitutos, se for o caso.

3.6.9. Serão consideradas não escritas as especificações, forma de execução do objeto ou qualquer outra condição, propostas pela licitante, que estejam em desacordo com o estipulado neste Edital.

3.7. Do cadastramento para acesso ao sistema de pregão eletrônico

3.7.1. Para acesso ao sistema eletrônico de licitação, a licitante deverá **minimamente** credenciar seu Representante Legal e efetuar a habilitação jurídica, no Cadastro Geral de Fornecedores - CAGEF, conforme orientações no Anexo II – Condições e documentos para habilitação.

3.7.1.1. O acesso ao sistema será feito pela licitante ou seu representante credenciado, mediante senha eletrônica, cujo fornecimento é de caráter pessoal e intransferível.

3.7.1.1.1. O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor ou gestor do sistema ou ao BDMG responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.7.1.1.2. O credenciamento para acesso ao sistema eletrônico de pregão implica a responsabilidade legal da licitante ou do seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico, sob pena de aplicação das sanções cabíveis.

3.7.1.1.3. A licitante se responsabiliza por todas as transações realizadas em seu nome, assumindo como firmes e verdadeiras as propostas e os lances efetuados por seu representante credenciado.

3.7.1.2. Orientações sobre o processo de cadastro da licitante e de seus representantes e outras informações pertinentes podem ser acessadas na página Cadastro Geral de Fornecedores – CAGEF do Portal de Compras – MG, site www.compras.mg.gov.br .

3.7.1.3. **ATENÇÃO:** o cadastramento prévio nos termos do item 3.7.1 ocorre sem qualquer interveniência do BDMG e sua não realização é condição impeditiva de participação na licitação.

3.7.2. A definição ou atualização da condição de Microempresa ou de Empresa de Pequeno Porte no CAGEF serão realizadas automaticamente por meio de integração entre os sistemas SIAD-MG e SIARE-MG, nos termos da Resolução Conjunta SEPLAG/SEF/JUCEMG Nº 9.576/2016.

3.7.2.1. A condição de empresa optante pelo Simples Nacional será confirmada pelo Pregoeiro, mediante consulta ao sítio do comitê Gestor do Simples Nacional.

3.8. Da proposta comercial

3.8.1. Da proposta original cadastrada no sistema

3.8.1.1. A licitante encaminhará a proposta original exclusivamente por meio do sistema, no site www.compras.mg.gov.br da rede mundial de computadores – internet, até a data e horário estabelecidos para abertura da sessão, mediante o preenchimento do respectivo formulário eletrônico e, se for o caso, o carregamento de arquivo com o detalhamento da proposta, observando obrigatoriamente o disposto no anexo relativo às condições e forma de apresentação da Proposta Comercial, indicado na folha de rosto deste Edital.

3.8.1.1.1. Até o momento da data e horário agendados para a abertura da sessão pública a proposta poderá ser reformulada e os documentos de proposta, se houver, poderão ser substituídos.

3.8.1.1.2. Na etapa relativa ao cadastramento da proposta original não haverá ordem de classificação, o que ocorrerá somente após o encerramento da fase competitiva a que se refere o item 6.1 deste edital.

3.8.1.1.3. A licitante declarará em campo próprio do sistema, sem prejuízo da exigência de outras declarações previstas em legislação específica, o cumprimento dos requisitos para habilitação e a conformidade de sua proposta com as exigências do edital de licitação.

3.8.1.1.3.1. A falsidade de alguma declaração das que trata o item 3.8.1.1.3 sujeitará a licitante às sanções previstas na legislação específica e neste edital.

3.8.1.1.4. Os documentos que compõem a proposta da licitante mais bem classificada somente serão disponibilizados para acesso público depois de definido o resultado do julgamento da proposta.

3.8.2. A proposta comercial conterá oferta firme e precisa, sem alternativas de preço ou quaisquer condições ou vantagens que induzam o julgamento, sob pena de ser considerada inválida.

3.8.2.1. Nas licitações para aquisição de bens ou contratação de serviços que incluam o fornecimento de bens, inclusive sistemas, o produto originalmente ofertado poderá ser substituído por outro que atenda todas as condições e requisitos mínimos estabelecidos, até o momento de apresentação da amostra, se exigida, ou aceitação final da proposta comercial.

3.8.2.2. Nas licitações que demandem a apresentação de planilha de composição de custos e formação de preços, o Pregoeiro poderá empreender diligências para dirimir dúvidas ou para adequação relacionada à superação de vícios sanáveis, nos termos do item 4.7.3 deste edital.

3.8.3. Será considerada inválida e, consequentemente, desclassificada a proposta que contiver vícios insanáveis, que não atender às exigências do Edital e seus anexos, que se vincular a outras propostas ou que contiver preço excessivo ou inexequível.

3.8.4. Serão considerados inclusos no preço proposto todos os custos, diretos e indiretos, lucro e ônus decorrentes da execução do objeto, tais como tributos, taxas, fretes, pessoal, equipamentos, materiais, publicidade e/ou quaisquer outros que venham a recair sobre o objeto desta licitação, não cabendo ao BDMG quaisquer custos adicionais, observados os termos deste Edital.

3.8.5. A validade da proposta será de, no mínimo, 60 (sessenta) dias corridos, contados a partir da data de apresentação ao BDMG do instrumento a que se refere o Anexo III do edital, item 2.4, devidamente preenchido e assinado.

3.8.6. A proposta, original ou apresentada em sede de negociação, é irretratável e sua retirada dará causa às sanções cabíveis previstas no item 10.

3.8.7. Um tutorial com orientações para o cadastramento de propostas pode ser consultado pelo link inserido AQUI, observadas as condições deste edital, Anexo III, item 1 e respectivos subitens.

3.9. Da documentação para habilitação

3.9.1. Para sua habilitação, será exigida da licitante a documentação especificada no anexo relativo às condições e documentos para Habilitação, conforme indicado na folha de rosto deste Edital, a serem encaminhados após a fase de lances e o encerramento da fase de negociação a que se refere o item 6.5 deste edital.

3.9.1.1. **ATENÇÃO:** a documentação de habilitação **NÃO SERÁ INCLUÍDA junto à proposta inicial, pelo campo "Arquivo(s) de descrição da proposta de preço - Proposta inicial",** mas por meio de funcionalidade própria do sistema e mediante convocação específica no âmbito da sessão pública.

3.9.2. Utilização do Certificado de Registro Cadastral - CRC

3.9.2.1. O Certificado de Registro Cadastral, CRC, emitido para a licitante pelo Sistema de Cadastro Geral de Fornecedores, CAGEF, da Secretaria de Estado de Planejamento e Gestão de Minas Gerais, SEPLAG/MG, será utilizado em substituição aos documentos por ele abrangidos.

3.9.2.2. Serão analisados no CRC somente os documentos exigidos para este certame, sendo desconsiderados todos os outros documentos do CRC, mesmo que estejam com a validade expirada.

3.9.2.3. Um tutorial com orientações para a obtenção do relatório CRC e ainda as certidões de regularidade junto ao CAFIMP e ao CEIS pode ser consultado pelo link inserido AQUI.

3.9.3. Da restrição na documentação de microempresas, empresas de pequeno porte e equiparados

3.9.3.1. Observado o disposto no item 3.6 deste edital, as microempresas (ME), empresas de pequeno porte (EPP) ou equiparadas deverão apresentar toda a documentação exigida para a habilitação, inclusive os documentos comprobatórios da situação fiscal, mesmo que estes contenham alguma restrição.

4. DAS REGRAS GERAIS DO PREGÃO

4.1. As normas que disciplinam esta licitação serão sempre interpretadas em favor da ampliação da disputa entre as licitantes, desde que não comprometam o interesse do BDMG, a finalidade e a segurança dos serviços objeto da licitação.

4.2. A participação nesta licitação implica:

I - na aceitação plena e irrevogável de todos os termos, cláusulas e condições deste Edital e seus anexos, a observância dos preceitos legais e regulamentares em vigor e a responsabilidade pela fidelidade e legitimidade das informações e dos documentos apresentados ao BDMG; e

II - no consentimento para publicação da documentação produzida no âmbito do processo licitatório, responsabilizando-se a licitante pelos ônus advindos da exposição dos dados de terceiros que houver nos documentos que apresentar.

4.3. Na ocorrência de divergência entre qualquer descrição e/ou informação contidas no portal Compras MG e neste edital e seus anexos, serão consideradas, para todos os efeitos, as contidas neste edital e seus anexos.

4.4. É responsabilidade da licitante acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, assumindo o ônus decorrente da sua não manifestação a quaisquer mensagens emitidas pelo Pregoeiro ou pelo sistema, ou de sua desconexão.

4.5. O BDMG não responderá pela desconexão de qualquer licitante com o sistema eletrônico e sua ocorrência não prejudicará a conclusão válida da sessão do pregão.

4.6. Da contagem de prazos

4.6.1. Na contagem dos prazos estabelecidos neste Edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.6.2. Para verificação dos prazos em dias úteis serão considerados os calendários de feriados e dias úteis de Belo Horizonte/MG bem como de feriados e dias úteis da FEBRABAN e os dias de atendimento ao público externo em expediente integral.

4.6.3. Os prazos definidos em horas serão contados em minutos – ex.: duas horas a partir de 10:30:40 terminarão às 12:30:00 – e os prazos definidos em minutos serão contados em segundos – ex.: dez minutos a partir de 10:30:40 terminarão às 10:40:40.

4.7. Das prerrogativas do Pregoeiro

4.7.1. O certame será realizado por Pregoeiro e equipe de apoio, conforme Portaria juntada aos autos desta licitação, aos quais não será devida qualquer remuneração ou comissão.

4.7.2. Mediante despacho fundamentado e acessível a todos, o Pregoeiro, no interesse do **BDMG**, poderá relevar omissões observadas nos documentos apresentados, bem como sanar erros ou falhas, atribuindo-lhes validade e eficácia para fins de classificação e habilitação, desde que não se contrarie a legislação vigente e não se comprometa a lisura do processo licitatório.

4.7.3. O Pregoeiro poderá, a seu exclusivo critério, para privilégio do interesse do **BDMG** e em qualquer fase da licitação, promover diligência destinada a suprir, complementar ou esclarecer a instrução do processo, podendo ser consultados os próprios licitantes, os respectivos emitentes de documentação e qualquer repositório de dados e informações válidos disponível, inclusive por meio eletrônico e nos autos de outros processos licitatórios do BDMG, devendo os documentos produzidos serem juntados ao processo.

4.7.3.1. Por dados e informações válidos tenham-se aqueles cuja autenticidade possa ser verificada pelo Pregoeiro.

4.7.3.2. Serão considerados autênticos os documentos apresentados em originais, cópias autenticadas em cartório e cópias autenticadas por comparação com os respectivos originais, inclusive mediante acesso ao pertinente sítio da internet e aos autos de outros processos licitatórios do **BDMG**, pelo Pregoeiro.

4.7.3.3. A indisponibilidade do respectivo sítio da internet, quando da aferição de validade das cópias de documentos digitais, não importará na imediata inabilitação da licitante, cuja contratação ficará condicionada à comprovação específica.

4.7.4. A não manifestação da licitante quando convocado para tanto, em qualquer fase da licitação, terá as seguintes implicações, conforme o caso:

a) a inércia quando chamada à negociação, para que encaminhe documentos ou informações, ou para que se manifeste acerca de qualquer questão proposta pelo Pregoeiro caracterizará desídia e implicará na desclassificação da proposta apresentada ou na inabilitação da licitante, conforme o caso;

b) a não interposição do recurso, nos termos do item 7 e respectivos subitens de edital, mediante funcionalidade do sistema que se refere a “Manifestação de intenção de recurso”, quando concedida a oportunidade para tanto, implicará na preclusão do direito de recorrer da licitante.

4.7.4.1. O não atendimento pelo licitante ao que for requerido pelo Pregoeiro em observância aos princípios e normas que regem o certame configurará comportamento inidôneo, passível de sancionamento nos termos do edital, item 10.1, inciso X, caso decorra de mera irresignação.

4.7.4.2. O atendimento parcial ao que foi demandado será considerado inércia para efeitos do que determina o item 4.7.4, alínea a.

5. DA SESSÃO PÚBLICA

5.1. Abertura da sessão pública

5.1.1. A sessão pública do pregão, realizada em ambiente virtual do Portal de Compras – MG na rede mundial de computadores - internet -, será aberta na data e no horário indicados na folha de rosto deste Edital, observado o horário de Brasília - DF.

5.1.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização da sessão na data marcada, esta será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e local aqui estabelecido, desde que não haja comunicação do Pregoeiro em contrário.

5.2. Suspensão da sessão pública

5.2.1. A sessão pública poderá ser suspensa pelo Pregoeiro em casos tais como

a) promoção de diligência que venha suprir, esclarecer ou complementar a instrução do processo;

b) promoção de diligência para obter dos setores competentes pareceres técnicos destinados a fundamentar suas decisões; e

c) dentre outros, a critério do Pregoeiro.

6. DOS PROCEDIMENTOS PARA SELEÇÃO DA MELHOR PROPOSTA

6.1. Da fase de lances

6.1.1. Aberta a sessão pública, o pregoeiro publicará os avisos pertinentes, mediante a ferramenta de chat do sistema, e dará início à fase competitiva, oportunidade em que as licitantes poderão encaminhar lances exclusivamente por meio do sistema.

6.1.2. No transcurso da sessão pública, serão divulgados, em tempo real, o valor e horário do melhor lance apresentado pelas licitantes bem como todas as mensagens trocadas no "chat" do sistema, sendo vedada a identificação da licitante.

6.1.3. O lance será ofertado pelo valor global ofertado**.**

6.1.3.1. O licitante somente poderá oferecer lance de valor inferior em relação ao último lance por ele ofertado, observado o intervalo mínimo de diferença de valores entre os lances que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta.

6.1.3.2. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao que cobrir a melhor oferta é de R$0,01 (um centavo).

6.1.4. A ordem de classificação das propostas será estabelecida segundo o critério de adjudicação definido para este certame.

6.1.4.1. Além do melhor preço, a licitante poderá disputar melhor colocação na ordem de classificação, por meio da oferta de lance inferior ao último por ela ofertado, não se lhe impondo, portanto, ofertar valor inferior ao menor lance registrado no sistema.

6.1.5. A licitante poderá solicitar ao Pregoeiro a exclusão do seu último lance, se proposto com erro manifesto.

6.1.5.1. Somente poderá ser realizada pelo Pregoeiro a exclusão solicitada mediante o comando próprio no sistema.

6.1.5.2. O pedido de exclusão poderá ou não ser atendido, cabendo a licitante o cuidado e a atenção necessários na propositura dos lances.

6.1.6. Caso a licitante não realize lances, será considerado o valor da proposta comercial originalmente apresentada, para efeito da classificação final.

6.1.7. No caso de desconexão do Pregoeiro, no decorrer da etapa competitiva do pregão, o sistema eletrônico permanecerá acessível às licitantes para a recepção dos lances.

6.1.7.1. O Pregoeiro, quando possível, dará continuidade à sua atuação no certame, sem prejuízo dos atos realizados.

6.1.7.2. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do pregão será suspensa e terá reinício somente após comunicação expressa aos participantes.

6.1.8. A etapa de envio de lances da sessão pública terá duração de 10 (dez) minutos e será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da fase competitiva.

6.1.8.1. A prorrogação automática da etapa de envio de lances, de que trata o item 6.1.8, supra, será de dois minutos e ocorrerá sucessivamente sempre que houver lances durante a prorrogação, inclusive quando se tratar de lances intermediários.

6.1.8.2. Na hipótese de não haver novos lances que ensejem a prorrogação automática ou durante o período de prorrogação, nos termos do item 6.1.8.1, a etapa competitiva será encerrada automaticamente, após o que haverá a aplicação do critério a que se referem o item 6.2 e respectivos subitens.

6.1.8.3. Encerrada a etapa competitiva sem prorrogação automática pelo sistema, nos termos do disposto no item 6.1.8.2, supra, o pregoeiro poderá, mediante justificativa, admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço.

6.1.8.4. Definida a proposta mais bem classificada, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% e se houver mais de dois licitantes, o pregoeiro poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.1.9. Caso haja empate após a etapa de envio de lances será realizada disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação.

6.1.9.1. Se não houver desempate será assegurada preferência, em igualdade de condições e sucessivamente, às empresas:

I - estabelecidas no território do Estado de Minas Gerais;

II - que invistam em pesquisa e no desenvolvimento de tecnologia no País;

III - que comprovem:

a) a prática de mudanças e substituições tecnológicas que reduzam o uso de recursos e as emissões por unidade de produção; ou

b) a implementação de medidas que reduzam as emissões de gases de efeito estufa e aumentem os sumidouros.

6.1.9.2. Na hipótese de persistir o empate após a aplicação dos critérios estabelecidos no subitem anterior a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

6.2. Do privilégio às ME, EPP ou equiparadas (empate ficto)

6.2.1. Observada a condição prevista no item 3.5 deste edital, em caso de empate ficto, entendido este como a situação em que as propostas apresentadas pelas microempresas (ME), empresas de pequeno porte (EPP) ou equiparadas possuam preços iguais ou até 5% (cinco por cento) superiores ao melhor preço, segundo o critério de adjudicação do objeto licitado, desde que ofertado por empresa não enquadrada como ME, EPP ou equiparada, será adotado o seguinte procedimento.

6.2.1.1. Obedecida a ordem de classificação das microempresas (ME), empresas de pequeno porte (EPP) ou equiparadas, o Pregoeiro convocará a detentora da proposta de menor valor dentre as que estejam na situação de empate ficto, para que apresente novo lance inferior ao melhor lance, no prazo de 05 (cinco) minutos, sob pena de preclusão do direito de preferência.

6.2.1.2. Realizado novo lance nos termos do item anterior, o Pregoeiro examinará a aceitabilidade deste quanto ao objeto e valor, decidindo motivadamente a respeito.

6.2.1.3. Sendo aceitável a nova oferta de preço, a confirmação das condições habilitatórias da ME, EPP ou equiparada obedecerá aos procedimentos previstos neste Edital.

6.3. Da verificação da conformidade da proposta

6.3.1. Obtida a classificação advinda da etapa de lances, o pregoeiro realizará a verificação da conformidade da proposta classificada em primeiro lugar, quanto à adequação às condições estabelecidas no edital, especialmente as do item 6.4 e respectivos subitens e do Anexo III, item 1 e respectivos subitens.

6.3.1.1. Caso entenda necessário, o pregoeiro acionará a funcionalidade do sistema relativa ao "envio de arquivo da proposta ajustada", para encaminhamento de documentação de detalhamento referente à proposta do licitante então mais bem classificado.

6.3.1.1.1. O licitante encaminhará a documentação requerida pelo pregoeiro no prazo de até 2 (duas) horas, prorrogável por mais duas horas, contado da publicação do respectivo aviso no chat do sistema.

6.3.1.1.1.1. A prorrogação de que trata o item 6.3.1.1.1 poderá ocorrer nas seguintes situações:

I – por solicitação do licitante, mediante justificativa aceita pelo pregoeiro;

II – de ofício, a critério do pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio dos documentos exigidos no edital para a verificação de conformidade de que trata o caput.

6.3.1.1.2. Analisadas a documentação apresentada para detalhamento da proposta original, conforme o edital, item 3.8.1.1, e a documentação requerida conforme o edital, item 6.3.1.1 e respectivos subitens, o pregoeiro poderá, a seu critério exclusivo, realizar a diligência que se fizer necessária, nos termos do edital, item 4.7.3.

6.3.1.1.2.1. O prazo para a apresentação da documentação relativa à diligência será definido pelo pregoeiro oportunamente, observado o princípio da igualdade.

6.3.1.1.3. Caso não haja documentação complementar a ser encaminhada, o pregoeiro encerrará o prazo e concluirá a análise de conformidade.

6.3.2. Será considerada inválida e, consequentemente, desclassificada a proposta que contiver vícios insanáveis ou que, quando presumidamente inexequível em relação ao valor ofertado advindo da fase de lances, não tiver a exequibilidade confirmada.

6.3.3. Verificada a conformidade a proposta será mantida classificada.

6.4. Da análise quanto à exequibilidade

6.4.1. Serão presumidas inexequíveis as propostas com valores globais inferiores a 70% (setenta por cento) do menor dos seguintes valores:

I – média aritmética dos valores das propostas resultantes da fase de lances, não consideradas as de valor excessivo; ou

II – valor estimado pelo **BDMG**.

6.4.2. Não serão consideradas inexequíveis as propostas resultantes da fase de lances que importarem em preços diferentes entre si em até 15%, quando apresentadas por todos ou por pelo menos três licitantes.

6.4.3. Caso entenda manifestamente inexequível a proposta, o Pregoeiro estabelecerá prazo para que o licitante demonstre a exequibilidade de seu preço.

6.4.3.1. Para demonstração da exequibilidade do preço ofertado será admitido planilha de composição de custos e formação de preços elaborada pelo próprio licitante ou qualquer outro critério apto adotado pelo Pregoeiro, em diligência.

6.4.3.2. Para efeito de demonstração da exequibilidade não se admitirá proposta que importe em ausência de lucro ao licitante em relação à prestação dos serviços advinda da licitação.

6.4.3.3. O licitante que permanecer inerte quando da convocação específica para que comprove a exequibilidade de sua proposta se sujeitará às sanções administrativas pela não manutenção da proposta previstas no item 10 deste edital.

6.4.4. Empreendida a análise pertinente, será considerada inexequível a proposta cuja viabilidade econômica não for verificada.

6.5. Da negociação com o então mais bem classificado

6.5.1. Verificada a conformidade da proposta então mais bem classificada, o pregoeiro poderá negociar, por meio do sistema e de forma pública e transparente, condições mais vantajosas para o **BDMG**, com o licitante então ocupante do primeiro lugar na ordem de classificação.

6.5.1.1. Negociado o preço ofertado, será concedido ao licitante então mais bem classificado o prazo mínimo de 2 (duas) horas para o encaminhamento da documentação de detalhamento desse preço, conforme a necessidade, observadas as condições do Anexo III do edital, item 2 e respectivos subitens.

6.5.1.1.1. Quando o objeto for composto de mais de um item de fornecimento e/ou serviço ou os custos forem também objeto de negociação os preços unitários finais serão menores ou iguais aos preços unitários da proposta inicial ou da proposta mais recentemente negociada.

6.5.1.1.2. No processo de negociação dos valores unitários, o Pregoeiro poderá encaminhar para a licitante mais bem classificada, bem como desta receber, planilhas preenchidas com os preços em ajustamento.

6.5.1.2. Caso não haja documentação a ser encaminhada, o pregoeiro encerrará o prazo e concluirá a fase de negociação.

6.5.2. Quando a proposta então mais bem classificada for desclassificada, a negociação poderá ser feita com os demais licitantes classificados, respeitada a ordem de classificação advinda da fase de lances, sendo utilizados, em caso de propostas intermediárias empatadas, os critérios de desempate definidos no item 6.1.9 deste edital.

6.5.3. A negociação poderá ser realizada pelo Pregoeiro em qualquer fase da licitação.

6.6. Da análise da documentação de habilitação

6.6.1. Aceita a proposta então mais bem classificada, o Pregoeiro passará à análise relativa à habilitação.

6.6.2. A documentação de habilitação será substituída pelo Certificado de Registro Cadastral, CRC, emitido pelo Sistema de Cadastro Geral de Fornecedores - CAGEF, da Secretaria de Estado de Planejamento e Gestão de Minas Gerais - SEPLAG/MG, da licitante, naqueles documentos por ele abrangidos, considerado ainda o que dispõem os itens 4.7.3 e 6.6.6 deste edital.

6.6.3. Os documentos exigidos para habilitação que não estejam contemplados no CAGEF serão enviados por meio do sistema, **mediante convocação específica pelo pregoeiro no âmbito da sessão pública**.

6.6.3.1. O licitante encaminhará a documentação requerida pelo pregoeiro no prazo de até 2 (duas) horas, prorrogável por mais duas horas, contado da publicação do respectivo aviso no chat do sistema.

6.6.3.1.1. A prorrogação de que trata o item 6.6.3.1 poderá ocorrer nas seguintes situações:

I – por solicitação do licitante, mediante justificativa aceita pelo pregoeiro;

II – de ofício, a critério do pregoeiro, quando constatado que o prazo estabelecido não é suficiente para o envio dos documentos exigidos no edital para a verificação de que trata o caput.

6.6.4. Em razão do que determina o edital, item 7.2, o Pregoeiro poderá, a seu exclusivo critério, disponibilizar aos licitantes, conforme mensagem via “chat” do sistema eletrônico, acesso alternativo à documentação de proposta e habilitação produzida até então, para que realizem a análise desses documentos em relação ao cumprimento do que determina o edital.

6.6.5. Caso pronuncie a inabilitação da licitante, o Pregoeiro examinará a aceitabilidade das propostas subsequentes, na ordem de classificação, verificando as condições de habilitação, até a apuração de uma proposta que atenda a este Edital.

6.6.6. Para fins de habilitação, os documentos cuja emissão for possível via acesso ao respectivo sítio da internet ou a qualquer outro repositório útil a tanto, inclusive os autos de outros procedimentos licitatórios do BDMG, poderão ser produzidos pelo Pregoeiro, que os juntará ao processo.

6.6.6.1. A possibilidade da consulta prevista no item 6.6.6 não constitui direito da licitante, e o BDMG não se responsabilizará pela eventual indisponibilidade dos meios necessários, hipóteses em que, em face do não saneamento das falhas constatadas, a licitante será declarada inabilitada.

6.6.7. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte será exigida nos termos do disposto no item 6.7 e respectivos subitens deste edital.

6.7. Da apresentação de documentação suplementar por ME, EPP ou equiparada

6.7.1. Desde que tenha suprido as demais condições de habilitação, caso a licitante mais bem classificada se enquadre na condição de ME, EPP ou equiparada apresente documento(s) comprobatório(s) de regularidade fiscal com restrição, será considerada habilitada pelo Pregoeiro, condicionada a habilitação à obtenção e comprovação da regularidade pertinente.

6.7.1.1. Neste caso, a sessão pública será suspensa para que, no prazo de 05 (cinco) dias úteis, contados do momento em que for declarada a vencedora do certame, comprove a obtenção da condição de regularidade, mediante o encaminhamento de cópia da certidão negativa ou positiva com efeitos de negativa específica, ao e-mail informado pelo Pregoeiro. O prazo é prorrogável por igual período, a critério exclusivo do BDMG, mediante requerimento escrito e fundamentado dirigido ao Pregoeiro, protocolado dentro do prazo original.

6.7.1.2. A não regularização do(s) documento(s), no prazo previsto ou concedido mediante prorrogação, implicará na inabilitação da licitante e decadência do direito à assinatura do contrato, sem prejuízo das sanções cabíveis, procedendo-se à convocação das demais licitantes, na ordem de classificação, ou à revogação da licitação.

6.8. Da possibilidade de apresentação de nova documentação

6.8.1. Quando todas as licitantes forem inabilitadas ou todas as propostas forem desclassificadas, o Pregoeiro, no interesse do BDMG, poderá fixar para as licitantes prazo para a apresentação de nova documentação ou de outras propostas escoimadas das causas referidas neste subitem, para realização de nova classificação e/ou de nova etapa de habilitação segundo as regras deste edital, conforme o caso.

6.9. Da classificação final e adjudicação do objeto

6.9.1. Após a identificação da melhor proposta, de acordo com o critério de adjudicação definido para o certame e que atenda a todas as exigências deste edital, será a licitante que a tiver proposto declarada vencedora da licitação.

6.9.2. No prazo máximo de 02 (dois) dias úteis contados da intimação específica, a licitante declarada vencedora deverá encaminhar ao BDMG:

a) a documentação de habilitação, em vias originais, cópias autenticadas ou cópias simples acompanhadas dos originais, neste caso sendo os originais posteriormente disponibilizados à licitante para retirada; e

b) o instrumento, devidamente preenchido e assinado, da proposta comercial adequada ao último valor ofertado, sendo os preços unitários finais menores ou iguais aos preços unitários da proposta inicial, acompanhado da planilha de detalhamento e dos demais documentos necessários, conforme o caso, segundo o disposto no anexo relativo às condições e forma de apresentação da Proposta Comercial indicado na folha de rosto deste edital.

6.10. Orientações para participação da sessão pública

6.10.1. Um tutorial sobre como participar da sessão pública – inclusive sobre como efetuar lances e interpor recursos – pode ser acessado mediante download pelo link inserido AQUI.

7. DOS RECURSOS

7.1. Ato contínuo ao término das fases:

a) de julgamento das propostas; e

b) de habilitação e declaração da vencedora do certame ou de certame fracassado

as licitantes poderão motivadamente interpor recurso, no prazo de 10 (dez) minutos, exclusivamente por meio do sistema eletrônico, em campo próprio.

7.1.1. **ATENÇÃO:** os recursos serão interpostos nos prazos específicos, segundo os atos e decisões a que se referirem, sendo intempestivos nos termos do item 7.4.1, alínea b:

a) os recursos relativos ao julgamento de propostas interpostos no prazo referente ao registro de recursos concernentes à habilitação e declaração de vencedor do certame;

b) os recursos relativos à fase de habilitação e à declaração de vencedor do certame interpostos no prazo referente à fase de julgamento de propostas.

7.1.2. **ATENÇÃO:** por uma característica do sistema o recurso interposto após o julgamento de propostas terá de ser novamente registrado, caso permaneça o interesse de recorrer, a cada vez que, em razão da inabilitação do licitante então mais bem classificado, o pregoeiro retornar à fase a que se refere o edital, item 6.3 e respectivos subitens.

7.1.2.1. A não reiteração do recurso nos termos do item 7.1.2 implicará na preclusão do direito de recorrer.

7.2. A interposição de recurso consiste na manifestação da licitante realizada no âmbito da sessão pública, tendo sido previamente disponibilizada a documentação produzida no âmbito da sessão pública e observados os pressupostos recursais, sendo o prazo posterior apenas para apresentação de razões e contrarrazões recursais.

7.2.1. As razões do(s) recurso(s) serão apresentadas em momento único, em campo próprio no sistema, no prazo de 3 (três) dias úteis, contados a partir da notificação acerca da admissão do(s) recurso(s), após a conclusão do juízo de admissibilidade a que se referem o item 7.4 e respectivos subitens deste edital, ficando os demais licitantes desde então intimados para apresentarem contrarrazões em igual número de dias, contados a partir do término do prazo do recorrente.

7.2.2. A apresentação das razões de recurso e das contrarrazões será feita exclusivamente por meio do sistema eletrônico, em campo próprio.

7.2.2.1. Serão consideradas como não escritas as razões recursais que não remetam diretamente às alegações registradas em sede de recurso, no âmbito da sessão pública.

7.2.2.2. A apresentação de documentos complementares cujos originais forem em papel e cuja validade e autenticidade não sejam passíveis de verificação em meio eletrônico ou digital será efetuada obrigatoriamente mediante protocolo junto ao Banco de Desenvolvimento de Minas Gerais S.A. – BDMG, na Rua da Bahia, nº 1.600, bairro de Lourdes, em Belo Horizonte/MG, CEP 30.160-907, no horário de 08h00 (oito horas) às 18h00 (dezoito horas), observados os prazos previstos no item 7.2.1.

7.3. O(s) recurso(s) será(ão) recepcionado(s) pelo Pregoeiro que apreciará sua admissibilidade, podendo reconsiderar sua decisão ou encaminhar o(s) recurso(s) à autoridade superior, que decidirá definitivamente sobre o provimento ou não do(s) recurso(s).

7.4. O juízo de admissibilidade dos recursos interpostos será realizado pelo pregoeiro após a declaração de vencedor do certame.

7.4.1. **ATENÇÃO:** **não será admitido** pelo Pregoeiro recurso em que se verifiquem ausentes os pressupostos da sucumbência, tempestividade, legitimidade, interesse e motivação, sendo:

a) sucumbência – referente à condição de não vencedor do recorrente, na licitação;

b) tempestividade – referente à interposição do recurso no prazo devido;

c) legitimidade – referente ao poder de representação necessário para a interposição do recurso, verificado quando do cadastramento no CAGEF;

d) interesse – referente à existência de efetivo benefício a ser auferido pelo recorrente no âmbito da licitação caso seja dado provimento ao recurso;

e) motivação – referente à indicação expressa, no campo específico do sistema, do(s) ato(s) ou decisão(ões) impugnadas e do(s) vício(s) nessa(s) decisão(ões) – exemplos:

"Recorro da decisão do Pregoeiro que considerou válida a proposta do licitante ..., em razão de a proposta não atender à condição do edital, Anexo ..., item ..."; ou

"Recorro da decisão do Pregoeiro que considerou habilitado o licitante ..., em razão de não comprovado o atendimento à condição de habilitação do edital, Anexo ..., item ...".

7.5. A falta de manifestação por qualquer das licitantes, mediante o sistema eletrônico, motivada e no prazo de 10 (dez) minutos contados da intimação específica, importará na preclusão do seu direito de recurso, caso em que Pregoeiro dará continuidade ao procedimento licitatório.

7.6. As licitantes poderão renunciar ao direito de recorrer ou ao prazo para apresentação de razões de recurso, mediante manifestação expressa por meio do sistema eletrônico, que será devidamente lavrada em ata.

7.6.1. Tendo havido a renúncia ao direito de recorrer ou ao prazo para apresentação de razões de recurso por todas as licitantes, o Pregoeiro passará imediatamente ao ato subsequente da licitação.

7.7. O recurso e as respectivas razões e contrarrazões, se houver, serão examinadas pelo Pregoeiro que reconsiderará ou manterá a decisão impugnada e, neste caso, submeterá o recurso à Autoridade Competente do BDMG, que decidirá de forma definitiva.

7.8. O acolhimento de recurso implicará invalidação apenas dos atos insuscetíveis de aproveitamento.

8. DA HOMOLOGAÇÃO

8.1. Inexistindo manifestação recursal, a autoridade competente do BDMG homologará o processo licitatório.

8.2. Julgados os recursos porventura interpostos e constatada a regularidade dos atos procedimentais, a autoridade competente do BDMG homologará o processo licitatório, adjudicando seu objeto para a licitante vencedora.

9. DA ASSINATURA DO INSTRUMENTO CONTRATUAL

9.1. Publicada a homologação da licitação e supridas as condições prévias de contratação do Anexo I deste edital, item 3, a licitante vencedora ou sua sucessora será convocada por meio do endereço eletrônico ou dos números de telefone que consignou no instrumento de sua proposta comercial, para que, em até 05 (cinco) dias úteis contados da convocação específica ou, na hipótese do item 9.2, alínea c, do recebimento do respectivo instrumento impresso, sob pena de decair o direito à contratação, assine o instrumento do contrato advindo da licitação, cuja minuta integra o Anexo IV deste edital.

9.2. A critério exclusivo do BDMG as vias do instrumento contratual serão:

a) digitais e assinadas mediante plataforma de assinaturas eletrônicas; ou

b) documentos natos do Sistema Eletrônico de Informações – SEI, do governo do Estado de Minas Gerais, assinados mediante procedimentos próprios desse sistema; ou

c) impressas em papel, sendo as assinaturas colhidas conforme o item 9.2.3 e respectivos subitens.

9.2.1. Sobre o instrumento contratual em vias digitais assinadas mediante plataforma de assinaturas eletrônicas

9.2.1.1. Orientações específicas acerca da assinatura serão dadas quando da convocação a que se refere o item 9.1.

9.2.2. Sobre o instrumento contratual em vias que são documentos natos SEI-MG assinados mediante procedimentos próprios desse sistema

9.2.2.1. Caso as vias do instrumento contratual sejam documentos natos SEI-MG, a licitante vencedora será convocada para que seu(s) representante(s) realize(m), em até 05 (cinco) dias úteis contados da convocação específica, o cadastramento como Usuário Externo no Sistema Eletrônico de Informações – SEI-MG, se ainda não cadastrado(s), mediante os procedimentos descritos na página específica do portal da Secretaria de Planejamento e Gestão do Governo de Minas Gerais na internet – https://www.mg.gov.br/planejamento/pagina/gestao-governamental/sei , no rol 'Outras informações', item 'Usuários externos'.

9.2.2.1.1. Um manual com instruções para o cadastramento pode ser consultado pelo endereço https://docs.google.com/document/d/1DCExqxTofGIt9nAN-ZDHuEUmQZ9wxxU8FFBGhKCEeHc/edit

9.2.2.2. A licitante vencedora comunicará ao BDMG, mediante e-mail encaminhado aos endereços pregao@bdmg.mg.gov.br e seibdmg@bdmg.mg.gov.br , a realização do cadastramento, quando da sua conclusão.

9.2.2.2.1. Caso o(s) representante(s) da licitante já esteja(m) previamente cadastrado(s) no SEI, deverá ser apresentado documento comprobatório de que tem(têm) poderes para a assinatura do instrumento contratual.

9.2.2.3. Realizados os procedimentos dos itens 9.2.2.1 a 9.2.2.2, a licitante vencedora será convocada para assinar os documentos no prazo estabelecido conforme o item 9.1.

9.2.3. Sobre o instrumento contratual em vias impressas em papel

9.2.3.1. No caso de encaminhamento das vias do instrumento em papel para a licitante vencedora, será considerada, para verificação do cumprimento do prazo a que se refere o item 9.1 a data da postagem na devolução da documentação, devidamente assinada, ao seguinte destinatário:

Banco de Desenvolvimento de Minas Gerais S.A. – BDMG
Núcleo de Contratos Administrativos
Rua da Bahia, 1.600, 2º andar – GP.LC
Lourdes
Belo Horizonte/MG
CEP 30.160-907

9.2.3.2. A critério exclusivo do BDMG, o prazo a que se refere o item 9.1, poderá ser prorrogado por igual período, uma única vez.

9.2.3.3. O instrumento contratual será assinado em duas vias originais.

9.3. Em caso de impossibilidade técnica a licitante poderá solicitar, mediante motivação devidamente justificada e em até um dia útil após a convocação a que se refere o item 9.1, a utilização de vias impressas em papel para a formalização da contratação, podendo o BDMG acatar ou não a solicitação.

9.4. Caso requerido no anexo relativo ao Termo de Referência deste Edital, a licitante vencedora deverá, mediante convocação específica e no prazo concedido pelo BDMG, comprovar o cumprimento das condições prévias à assinatura do instrumento contratual.

9.5. O não comparecimento da licitante vencedora convocada no prazo fixado pelo BDMG importará na perda do direito à assinatura do instrumento contratual.

9.6. Caso a licitante vencedora não apresente situação regular na ocasião da assinatura do contrato ou se recuse a assiná-lo será sucedida por outro licitante, obedecida a ordem de classificação advinda da licitação.

9.7. Nas hipóteses dos itens 9.5 e 9.6 o procedimento do pregão será reaberto para o exame das ofertas e qualificação das licitantes, obedecida a ordem de classificação, até a apuração de uma proposta que atenda ao edital, sendo a respectiva licitante declarada vencedora, e, não havendo recurso, ser-lhe-á adjudicado o objeto, cabendo, a esse procedimento, conforme o caso, os preceitos contidos nos itens 7 e 8 deste edital.

9.8. Será admitido a assinar o instrumento contratual apenas a licitante que atender às exigências de habilitação previstas neste edital, inclusive as prévias de contratação, devendo mantê-las durante toda a vigência do contrato.

9.9. A classificação resultante da licitação será mantida durante toda a vigência do contrato ela advindo.

9.10. Caso a licitante sucessora seja convocada em prazo posterior ao término da vigência de sua proposta comercial, os preços serão atualizados pelo índice IPCA acumulado a partir da data de apresentação da respectiva proposta.

10. DAS PENALIDADES

10.1. Poderá ser aplicada a pena de suspensão de participação em licitação e contratação com o BDMG, por até 02 (dois) anos, para a licitante que:

I – tenha sofrido condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

II – tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

III – demonstre não possuir idoneidade para contratar com o BDMG em virtude de atos ilícitos praticados;

IV – convocado dentro do prazo de validade da sua proposta, não celebrar o contrato;

V – deixar de entregar a documentação exigida para o certame;

VI – apresentar documentação falsa exigida para o certame;

VII – ensejar o retardamento da execução do objeto da licitação;

VIII – não mantiver a proposta;

IX – falhar ou fraudar na execução do contrato;

X – comportar-se de modo inidôneo, inclusive com a prática de atos lesivos à Administração Pública previstos na Lei Federal nº 12.846/2013.

10.2. A recusa injustificada do adjudicatário em assinar o instrumento contratual, aceitar ou retirar os instrumentos ou equivalentes, dentro do prazo estabelecido pelo BDMG, além de ensejar outras cominações legais, sujeitá-lo-á, garantida a ampla defesa, à aplicação de multa no mesmo percentual definido para a multa compensatória prevista na cláusula de penalidades da minuta do instrumento contratual anexa a este edital.

10.3. Pelo atraso, inexecução total ou parcial no cumprimento do objeto a ser contratado, garantida a ampla defesa, a licitante contratada ficará sujeita às sanções previstas na cláusula de penalidades da minuta do instrumento contratual, conforme anexo pertinente deste Edital.

11. DISPOSIÇÕES GERAIS

11.1. Em razão do que determina a Lei Geral de Proteção de Dados, o acesso aos autos do processo licitatório, no qual há dados pessoais em documentos que o compõem, será por requisição expressa, mediante a apresentação de instrumento de declaração de compromisso devidamente preenchido e assinado e com a qualificação do interessado, nos seguintes termos:

I – interessado pessoa física: "Eu, <NOME>, inscrição nº <Nº DO CPF> no CPF, residente na <ENDEREÇO COMPLETO>, endereço eletrônico <ENDEREÇO DE E-MAIL> solicito que me seja encaminhada via e-mail cópia dos autos do processo licitatório edital BDMG-19/2026. Para tanto, comprometo-me a manter sigilo em relação aos dados pessoais de terceiros constantes na documentação e declaro que esses dados não serão compartilhados e não serão utilizados, de qualquer forma e em qualquer medida, para o que não se refira objetivamente ao processo licitatório edital BDMG-19/2026".

II – interessado pessoa jurídica: "A <NOME EMPRESARIAL>, inscrição nº <Nº DO CNPJ> no CNPJ, com endereço na <ENDEREÇO COMPLETO> e endereço eletrônico <ENDEREÇO DE E-MAIL>, solicita, na pessoa de seu(s) representante(s) <NOME DO REPRESENTANTE LEGAL>, inscrição no CPF nº <Nº DO CPF>, residente na <ENDEREÇO COMPLETO> e e-mail <ENDEREÇO DE E-MAIL>, signatário(s) desta declaração, que lhe seja encaminhada via e-mail cópia dos autos do processo licitatório edital BDMG-19/2026. Para tanto, compromete-se com a manutenção do sigilo em relação aos dados pessoais de terceiros constantes nos autos do processo licitatório edital BDMG-19/2026 e declara que esses dados não serão compartilhados e não serão utilizados, de qualquer forma e em qualquer medida, para o que não se refira objetivamente ao processo licitatório edital BDMG-19/2026".

11.2. O interessado pessoa física apresentará junto ao instrumento a que se refere o item 11.1, inciso I, documento de identificação civil válido (RG, CNH, ou outro conforme a lei) e CPF.

11.3. O interessado pessoa jurídica apresentará junto ao instrumento a que se refere o item 11.1, inciso II, documento de identificação civil válido (RG, CNH, ou outro conforme a lei) e CPF do representante legal e comprovação dos poderes de representação.

11.4. O acesso aos autos poderá ser feito também presencialmente, mediante agendamento pelo e-mail pregao@bdmg.mg.gov.br , quando o interessado apresentará os respectivos instrumentos e documentos referidos nos itens 11.1 a 11.3.

12. FORO

12.1. Para dirimir as questões oriundas do presente Edital, não resolvidas na esfera administrativa, é competente o Foro da Comarca de Belo Horizonte, MG, por mais privilegiado que outro seja.

Belo Horizonte, 06 de novembro de 2026.

Evandro Dolabella Melo
Pregoeiro do BDMG

ANEXO I – TERMO DE REFERÊNCIA

1. OBJETO

1.1. Contratação de empresa especializada na prestação de serviços gerenciados de Centro de Operações de Segurança (SOC), em regime de operação contínua 24x7x365 (24 horas por dia, 7 dias por semana, 365 dias por ano), compreendendo os seguintes serviços:

- **Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR)**: serviço gerenciado de monitoramento contínuo, triagem, investigação, classificação, priorização, contenção e resposta a incidentes de segurança cibernética do ambiente de TI do BDMG, 24x7x365 (24 horas por dia, 7 dias por semana, 365 dias por ano);
- **Caça a Ameaças Cibernéticas (Threat Hunting)**: serviço continuado de busca proativa, iterativa e orientada por hipóteses de ameaças já presentes no ambiente do BDMG e ainda não identificadas pelos controles de detecção vigentes, orientado pelo framework de cibersegurança MITRE ATT&CK e pela inteligência de ameaças, executado por campanhas estruturadas de periodicidade definida e por campanhas reativas acionadas por gatilho, com conversão obrigatória de cada achado e de cada lacuna de visibilidade em nova detecção versionada no ambiente do Banco;
- **Inteligência de Ameaças (Threat Intelligence):** serviço continuado de integração, curadoria, análise, enriquecimento e disseminação de inteligência sobre ameaças cibernéticas relevantes ao BDMG e ao setor financeiro, executado por equipe própria e distinta da equipe de Caça a Ameaças, contemplando a integração de feeds nos padrões STIX e TAXII sem custo adicional de ferramenta, a análise periódica do cenário de ameaças, o mapeamento de agentes de ameaça e a modelagem de ameaças com referência aos frameworks MITRE ATT&CK e STRIDE, a gestão do ciclo de vida dos indicadores de comprometimento e a produção de relatórios periódicos compartilhados de forma estruturada com as frentes de Caça a Ameaças e de Engenharia de Detecção**;**
- **Engenharia de Detecção e Otimização do SIEM**: serviço continuado de administração, configuração, sustentação e evolução da plataforma de SIEM (Security Information and Event Management) Microsoft Sentinel do BDMG, contemplando a integração de fontes de dados de eventos de segurança a manutenção de conectores, o desenvolvimento e o ajuste de regras de correlação, a criação de playbooks e automações, a manutenção das consultas de investigação (hunting queries) em suporte à frente de Caça a Ameaças (Threat Hunting), a gestão da saúde da solução, a otimização de desempenho e do custo de ingestão e o suporte técnico à operação de monitoramento de segurança;
- **Gestão de Vulnerabilidades**: serviço continuado de identificação, análise, priorização, tratamento e monitoramento de vulnerabilidades de segurança nos ativos de TI do BDMG, incluindo a realização de varreduras autenticadas e não autenticadas, a análise dinâmica de aplicações web, a priorização baseada em risco para o negócio, a orquestração e o acompanhamento da remediação e a validação das correções aplicadas, com o objetivo de reduzir a exposição a ameaças cibernéticas por meio da correção ou da mitigação tempestiva das vulnerabilidades identificadas.

A contratação pretendida será feita em lote único, com pagamentos mensais condicionados ao cumprimento dos níveis de serviço (SLAs) e dos indicadores de desempenho estabelecidos. Eventuais descumprimentos poderão resultar em descontos proporcionais (glosas) na remuneração da CONTRATADA. O objeto compreende dois escopos sucessivos e distintos: o escopo de IMPLANTAÇÃO, com prazo de até 2 (dois) meses e sem remuneração específica, e o escopo de OPERAÇÃO, de prestação continuada, remunerado em 12 (doze) parcelas mensais. O contrato terá, por isso, vigência inicial de 14 (quatorze) meses e poderá ser prorrogado, quanto ao escopo de OPERAÇÃO, por se tratar de serviço contínuo, até o limite de 60 (sessenta) meses contados de sua celebração, observado que o último período contratual será de 10 (dez) meses.

A execução observará, em todos os seus aspectos técnicos, operacionais e de governança, o Anexo IV-A – Termo de Referência – Requisitos, integrante do Anexo IV – Minuta do Instrumento Contratual.

Item	Descrição	Unidade	Quantidade total
1	Serviço Gerenciado de Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR)	Serviço Mensal	12 (doze)
2	Serviço de Gestão de Vulnerabilidades	Serviço Mensal	12 (doze)
3	Licenças de uso de solução de Gestão de Vulnerabilidades com Gerenciamento de Patches, por 12 (doze) meses	Ativos monitorados	1.200 (mil e duzentos)

O detalhamento integral do objeto e as especificações técnicas constam do Anexo IV-A – Termo de Referência – Requisitos, que integra o Anexo IV – Minuta do Instrumento Contratual e vincula a contratação.

1.2. Demais condições estabelecidas conforme Anexo IV – Minuta do Instrumento Contratual.

2. VALOR DE REFERÊNCIA

2.1. O valor de referência estimado e máximo aceitável para a presente contratação é de R$ 2.236.203,60 (Dois milhões, duzentos e trinta e seis mil, duzentos e três reais e sessenta centavos), correspondente ao primeiro período contratual, de 14 (quatorze) meses, assim composto: até 2 (dois) meses de implantação, não remunerada de forma separada, e 12 (doze) meses de operação continuada.

A etapa de implantação terá os custos integralmente diluídos nas 12 (doze) parcelas mensais de operação, na forma do subitem 1.1.2 do Anexo IV-A – Termo de Referência – Requisitos e do subitem 7.1.1 do Anexo IV – Minuta do Instrumento Contratual.

Nas prorrogações, que alcançarão exclusivamente o escopo de operação, o valor será apurado sobre 12 (doze) parcelas mensais de operação por período, observado que o último período contratual será de 10 (dez) meses, de modo a não exceder o limite de 60 (sessenta) meses contados da celebração do contrato.

Item	Descrição	Unidade	Quantidade total	Valor máximo mensal/unitário	Valor máximo anual
1	Serviço Gerenciado de Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR)	Serviço Mensal	12 (doze)	R$ 110.658,61	R$ 1.327.903,32
2	Serviço de Gestão de Vulnerabilidades	Serviço Mensal	12 (doze)	R$ 24.368,69	R$ 292.424,28
3	Licenças de uso de solução de Gestão de Vulnerabilidades com Gerenciamento de Patches, por 12 (doze) meses	Ativos monitorados	1.200 (mil e duzentos)	R$ 513,23	R$ 615.876,00
TOTAL					R$ 2.236.203,60

3. CONDIÇÕES PRÉVIAS À CONTRATAÇÃO

3.1. Como condição prévia à assinatura do contrato advindo da licitação, será conferida a condição do licitante no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual – CAFIMP.

3.2. A licitante adjudicatária será convocada para assinar o instrumento contratual em até 05 (cinco) dias úteis, com eventual prorrogação a critério do BDMG, devendo apresentar os dados dos representantes legais, que assinarão o instrumento, observadas as condições do edital BDMG-19/2026, item 9 e respectivos subitens.

3.2.1. Os poderes de representação serão comprovados pela licitante adjudicatária mediante a apresentação da seguinte documentação, conforme o caso:

a) estatuto ou contrato social em vigor consolidado, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores, devidamente registrados;

b) ato constitutivo, devidamente registrado, no caso de sociedade civil ou não empresária, acompanhado de prova de investidura ou nomeação da diretoria em exercício;

c) outros documentos necessários à efetiva comprovação dos poderes de representação, segundo a realidade da licitante adjudicatária.

3.2.2. A convocação se dará por e-mail ao endereço eletrônico indicado pela licitante adjudicatária no instrumento de sua proposta comercial.

3.3. Publicada a homologação da licitação, a licitante adjudicatária será convocada para, no mesmo prazo referente à assinatura do contrato advindo da licitação, entregar ao BDMG:

3.3.1. declaração formal indicando a existência ou não, dentre aqueles que compõem sua participação societária, seus administradores ou seus prepostos, de pessoa exposta politicamente (PEP), ou de pessoa que esteja na condição de representante, familiar ou estreito colaborador de PEP, para cumprimento do art. 56 da Circular BACEN nº 3.978, de 23 de janeiro de 2020.

3.3.2. A exigência do subitem 3.3.1 constitui condição prévia à contratação, a ser cumprida exclusivamente pela licitante adjudicatária após a homologação do certame, e não requisito de habilitação, não sendo exigível das demais licitantes nem na fase de habilitação.

3.4. Como condição prévia à assinatura do contrato advindo da licitação, a licitante adjudicatária deverá comprovar a equipe técnica mínima e as respectivas certificações, na forma do item 7 do Anexo IV-A – Termo de Referência – Requisitos, mediante apresentação de diplomas, certificados vigentes e comprovação de vínculo profissional (CTPS, contrato de trabalho, contrato de prestação de serviços ou ato societário).

4. DEMAIS CONDIÇÕES

4.1. Expressas nos demais anexos deste edital BDMG-19/2026.

ANEXO II – CONDIÇÕES E DOCUMENTOS DE HABILITAÇÃO

1. Sobre o cadastro no Portal de Compras MG

1.1. Orientações sobre o processo de cadastro da licitante e de seus representantes e outras informações pertinentes podem ser acessadas na página Cadastro Geral de Fornecedores – CAGEF do Portal de Compras – MG, site www.compras.mg.gov.br, ou pela Central de Atendimento aos Fornecedores, mediante o telefone (31) 3916-9755 e o e-mail cadastro.fornecedores@planejamento.mg.gov.br.

2. Os seguintes documentos serão apresentados pelo licitante então mais bem qualificado, mediante convocação específica pelo pregoeiro, para sua habilitação, qualquer que seja o lote pretendido, tendo em conta o que prevê o edital, item 4.7.3, e que o Certificado de Registro Cadastral, CRC, emitido ao licitante mediante o Sistema de Cadastro Geral de Fornecedores, CAGEF, da Secretaria de Estado de Planejamento e Gestão de Minas Gerais, SEPLAG/MG, será utilizado em substituição aos documentos por ele abrangidos, e que não será exigida a comprovação de atendimento a condição suspensa por determinação legal, neste caso consideradas as disposições do edital, item 3.6.8.

2.1. Um tutorial com orientações para a obtenção do relatório CRC e das certidões de regularidade junto ao CAFIMP e ao CEIS pode ser consultado pelo link inserido AQUI.

2.2. Regularidade jurídica

2.2.1. Registro comercial, no caso de empresa individual;

2.2.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores, devidamente registrados. Em qualquer caso, tais documentos deverão estar acompanhados de suas alterações ou consolidação;

2.2.3. Ato constitutivo, devidamente registrado, no caso de sociedade civil ou não empresária, acompanhado de prova de investidura ou nomeação da diretoria em exercício;

2.2.4. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

2.2.5. Prova de que a licitante não consta no Cadastro de empregadores que tenham submetido trabalhadores a condições análogas à de escravo, conforme a Portaria MTPS/MMIRDH nº 4, de 11 de maio de 2016.

2.2.5.1. A Lista Suja do Trabalho Escravo publicada pelo Ministério do Trabalho e Emprego é documento apto à comprovação a que se refere o item 2.2.5.

2.3. Regularidade fiscal

2.3.1. Prova de inscrição regular no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda, CNPJ/MF, no caso de pessoa jurídica ou pessoa física com inscrição no CNPJ (MEI/EI);

2.3.2. Prova de regularidade de situação para com a Seguridade Social e perante a Fazenda Nacional, por meio da “Certidão Conjunta Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União” ou "Certidão Conjunta Positiva com Efeitos de Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União", nos termos da Portaria RFB/PGFN nº 1.751, de 02/10/2014;

2.3.3. Prova de regularidade perante a Fazenda Estadual por meio de certidão negativa de débitos ou positiva com efeitos negativos, emitida pela Secretaria de Estado da Fazenda do domicílio da licitante;

2.3.4. Certificado de regularidade junto ao FGTS, expedido pela Caixa Econômica Federal, caso seja pessoa jurídica, ou, no caso de licitante Pessoa Física sem inscrição no CNPJ, declaração de que não mantém empregado.

2.3.5. Prova de regularidade relativa a Débitos Trabalhistas, por meio da “Certidão Negativa de Débitos Trabalhistas”, nos termos da Lei nº 12.440/2011 e ao Ato CGJT nº 1, de 21 de janeiro de 2022.

2.4. Qualificação econômico-financeira

2.4.1. Certidão negativa de falência emitida pelo distribuidor da comarca onde se encontre a sede da licitante e expedida com antecedência máxima de 180 (cento e oitenta) dias, salvo se a própria certidão estabelecer prazo de validade diverso, ou comprovação, por qualquer meio apto, de encontrar-se em processo de recuperação judicial.

2.4.1.1. No caso de comarcas com mais de um cartório distribuidor, deverão ser apresentadas as certidões de cada distribuidor.

2.4.1.2. A certidão negativa cível que abarque ações de falência poderá ser apresentada em substituição à requerida no subitem 2.4.1 acima, observadas as mesmas condições de emissão e desde que possível a verificação pertinente junto ao órgão emissor.

2.4.2. Comprovação de Capital Circulante Líquido (CCL) ou Capital de Giro (Ativo Circulante – Passivo Circulante) de, no mínimo, 10% (dez por cento) do valor de referência estimado e máximo aceitável para a contratação.

2.4.2.1. O Capital Circulante Líquido será apurado com base no balanço patrimonial e nas demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, vedada a substituição por balancetes ou por balanços provisórios.

2.4.2.2. As sociedades constituídas no exercício em curso poderão comprovar o requisito mediante balanço de abertura.

2.5. Qualificação técnica

2.5.1. Atestado(s) de capacidade técnica, em nome da licitante, emitido(s) por instituição(ões) financeira(s) de direito público ou privado que comprove(m) a prestação de serviços gerenciados

de Centro de Operações de Segurança da Informação (SOC), em regime ininterrupto 24x7x365, incluindo, no mínimo, os itens a seguir:

2.5.1.1. Serviço Gerenciado de Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR), operado em ambiente com capacidade de processamento de eventos de segurança de, no mínimo, 800 EPS (Events Per Second) ou 60 GB (sessenta gigabytes) de logs/dados por dia;

2.5.1.2. Serviço de Gestão de Vulnerabilidades em ambiente computacional contendo, no mínimo, 500 (quinhentos) ativos de TI.

2.5.2. Atestado(s) de capacidade técnica, em nome da licitante, emitido(s) por instituição participante do Sistema de Pagamentos Brasileiro (SPB), comprovando que a licitante presta ou prestou serviços de Centro de Operações de Segurança da Informação (SOC), abrangendo o monitoramento, a detecção e a resposta a incidentes cibernéticos, prestados sobre o ambiente tecnológico que suporta ou suportava a participação da emitente em sistema integrante do Sistema de Pagamentos Brasileiro, pelo período mínimo de 12 (doze) meses ininterruptos.

2.5.2.1. Para fins de comprovação do requisito previsto no subitem 2.5.2, considera-se participante do Sistema de Pagamentos Brasileiro (SPB) a pessoa jurídica que, durante o período de prestação dos serviços considerado para o atendimento daquele subitem, figurava como participante de sistema integrante do SPB destinado à transferência de fundos, à compensação ou à liquidação, operado ou autorizado pelo Banco Central do Brasil, incluindo o Sistema de Transferência de Reservas (STR), o Sistema de Pagamentos Instantâneos (SPI), o Sistema de Liquidação Diferida das Transferências Interbancárias de Ordens de Crédito (SILOC) e o Sistema de Transferência de Fundos (Sitraf), bem como os sistemas de compensação e de liquidação operados por câmaras ou prestadores de serviços de compensação e de liquidação sujeitos à disciplina da Lei nº 10.214, de 27 de março de 2001.

2.5.2.2. A condição prevista no subitem 2.5.2.1 poderá ser comprovada por qualquer meio idôneo, inclusive mediante indicação, no próprio atestado, do número de identificação da instituição no Sistema de Pagamentos Brasileiro (ISPB) ou do sistema de que participa ou participava, cabendo ao BDMG verificar as informações nas relações e demais fontes oficiais disponibilizadas pelo Banco Central do Brasil.

2.5.2.3. Um único atestado poderá ser utilizado para a comprovação simultânea dos requisitos dos subitens 2.5.1 e 2.5.2, desde que contenha todos os elementos exigidos em cada um deles.

2.5.3. Atestado(s) de capacidade técnica, em nome da licitante, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a prestação de serviços de operação de plataforma de SIEM Microsoft Sentinel, executados em ambiente com capacidade de processamento de eventos de segurança de, no mínimo, 800 EPS (Events Per Second) ou 60 GB (sessenta gigabytes) de logs/dados por dia.

2.5.4. Os atestados de que tratam os subitens 2.5.1 a 2.5.3 observarão as seguintes regras:

2.5.4.1. Para fins de comprovação dos quantitativos de EPS, GB ou ativos de TI exigidos nos subitens 2.5.1.1, 2.5.1.2 e 2.5.3, será admitido o somatório de atestados, desde que cada atestado comprove a execução integral dos serviços descritos e que os períodos de prestação

atestados sejam concomitantes, de modo a demonstrar a capacidade de atendimento simultâneo dos quantitativos somados.

2.5.4.2. O(s) atestado(s) apresentado(s) para comprovação do atendimento aos subitens 2.5.1, 2.5.2 e 2.5.3 deverá(ão) conter dados aptos a identificar o(s) emitente(s) e possibilitar contato para validação e diligência (nome, cargo, telefone e e-mail institucional do signatário).

2.5.4.3. Não será(ão) aceito(s) atestado(s) de capacidade técnica emitido(s) pela própria licitante para comprovação do atendimento aos subitens 2.5.1, 2.5.2 e 2.5.3.

2.5.4.4. Não será(ão) aceito(s) atestado(s) de capacidade técnica emitido(s) por empresa do mesmo grupo econômico da licitante para comprovação do atendimento aos subitens 2.5.1, 2.5.2 e 2.5.3.

2.5.5. Comprovação de que a licitante possui certificação ISO/IEC 27001:2022 ou ABNT NBR ISO/IEC 27001:2022, ou versão posterior que a substitua, cujo escopo abranja a prestação de serviços de Centro de Operações de Segurança (SOC).

2.5.5.1. O documento comprobatório da certificação deverá ser apresentado em nome da licitante, com validade vigente na data de apresentação e com indicação do escopo certificado, sendo facultado ao BDMG promover diligência destinada a esclarecer ou complementar informações, inclusive junto ao organismo certificador.

2.5.5.2. Não serão aceitos atestados e/ou declarações em substituição à certificação exigida.

2.5.5.3. Atende ao requisito de escopo o certificado que descreva a prestação de serviços de SOC, de MDR ou de serviços gerenciados de segurança que compreendam o monitoramento, a detecção e a resposta a incidentes cibernéticos, ainda que não empregue a sigla “SOC”. Não atende ao requisito o certificado cujo escopo se restrinja a unidades, processos ou serviços da licitante distintos dessas atividades.

2.5.6. Declaração emitida pelo fabricante da solução de gestão de vulnerabilidades ofertada, ou de seu distribuidor oficial no Brasil, atestando que a licitante está autorizada a comercializar e a prestar suporte à solução no território nacional durante a vigência contratual.

2.5.6.1. Caso o módulo de Patch Management, o de Policy Compliance ou o de análise dinâmica de aplicações web seja de fabricante distinto do da solução de gestão de vulnerabilidades, inclusive em regime de OEM, a declaração será exigida também do respectivo fabricante ou de seu distribuidor oficial no Brasil, abrangendo o módulo correspondente.

2.5.7. Declaração de que, na data da assinatura do contrato, caso venha a ser a vencedora, a licitante comprovará dispor da equipe mínima e das certificações previstas no item 7 do Anexo IV-A – Termo de Referência – Requisitos, mediante apresentação de diplomas, certificados vigentes e vínculo profissional (CTPS, contrato de trabalho, contrato de prestação de serviços ou ato societário).

2.5.7.1. A comprovação de equipe e das respectivas certificações não será exigida na fase de habilitação, mas na assinatura do contrato.

2.5.7.2. As certificações da equipe mínima deverão permanecer vigentes durante toda a execução contratual, admitido o prazo de até 3 (três) meses para reapresentação em caso de expiração, na forma do subitem 7.18 do Anexo IV-A – Termo de Referência – Requisitos.

2.5.8. Documentação oficial do fabricante da solução que demonstre o atendimento aos itens 5.1 a 5.81 do Anexo IV-A, conforme item 5.82 do mesmo Anexo.

2.6. O Certificado de Registro Cadastral, CRC, emitido ao licitante mediante o Sistema de Cadastro Geral de Fornecedores, CAGEF, da Secretaria de Estado de Planejamento e Gestão de Minas Gerais, SEPLAG/MG, será utilizado em substituição aos documentos por ele abrangidos.

2.6.1. Serão analisados no CRC somente os documentos exigidos para este certame, sendo desconsiderados todos os outros documentos do CRC, mesmo que estejam com a validade expirada.

2.6.2. Os documentos abrangidos pelo CRC, exigidos para este certame, que estiverem vencidos e cuja emissão via acesso público ao respectivo site na internet não seja possível, deverão ser encaminhados ao Pregoeiro quando da convocação específica.

3. Do encaminhamento da documentação original de habilitação, conforme o item 6.9.2 do edital

3.1. A documentação de habilitação que for em papel, em vias originais, cópias autenticadas ou cópias simples acompanhadas dos originais, neste caso sendo os originais posteriormente disponibilizados ao licitante para retirada, será entregue em envelope que contenha em seu anverso a referência ao nome, número do certame, os dizeres "Habilitação", a identificação do Lote pretendido e a identificação do licitante, conforme o seguinte modelo:

Pregão BDMG-19/2026
HABILITAÇÃO
<nome do licitante>

ANEXO III – CONDIÇÕES E FORMA DE APRESENTAÇÃO DAS PROPOSTAS COMERCIAIS

1. Da proposta original, preenchida em formulário eletrônico no portal Compras MG.

1.1. Será registrado no campo relativo a valor do formulário eletrônico de propostas do sistema o valor ofertado correspondente ao primeiro período contratual, conforme Anexo I, item 2.1.

1.1.1. **ATENÇÃO:** na elaboração da proposta original os licitantes considerarão que os valores individuais relativos à proposta final negociada após a fase de lances serão obtidos mediante a aplicação linear do desconto a que corresponde o valor global final negociado em relação ao valor global originalmente ofertado, nos termos do item 2.2 deste anexo.

1.2. **ATENÇÃO:** o valor global ofertado será determinado mediante a utilização obrigatória do arquivo XLSX de detalhamento de proposta disponível mediante download pelo endereço https://tinyurl.com/4jrfhbve .

1.2.1. O arquivo XLSX de detalhamento de proposta será encaminhado quando do registro da proposta original no sistema, devidamente preenchido e mediante a funcionalidade "Arquivo(s) de descrição da proposta de preço - Proposta inicial", conforme a figura abaixo:



1.2.1.1. **ATENÇÃO:** o não encaminhamento do arquivo de detalhamento do preço global originalmente proposto ou o arquivo que contenha vício insanável darão causa à desclassificação da proposta.

1.3. **ATENÇÃO:** não será incluída documentação de habilitação junto à proposta.

1.3.1. A documentação de habilitação será apresentada pelo licitante mediante convocação específica, no âmbito da sessão pública, nos termos do edital, item 6.6 e respectivos subitens.

1.4. A proposta comercial conterá oferta firme e precisa, sem alternativas de preço ou quaisquer condições ou vantagens que induzam o julgamento.

1.5. Os valores serão registrados em moeda corrente no País e grafados com apenas duas casas decimais para todos os campos a serem preenchidos.

1.6. No preço proposto, estarão incluídos todos os custos, diretos e indiretos, lucro e ônus decorrentes da prestação de serviços, tais como tributos, taxas, custos de deslocamentos ou quaisquer outros que venham a recair sobre o objeto da licitação, não cabendo ao BDMG quaisquer custos adicionais, observados os termos deste Edital.

1.7. Quaisquer custos, diretos ou indiretos, e ônus omitidos da proposta comercial ou incorretamente cotados serão considerados inclusos no preço, não sendo admitidos pleitos de acréscimo a esse ou a qualquer título, devendo o objeto licitado ser executado sem qualquer ônus adicional para o BDMG.

2. Da apresentação do instrumento impresso da proposta pelo vencedor da licitação e documentos e/ou informações complementares pertinentes.

2.1. A proposta comercial do licitante vencedor será entregue adequada ao último valor ofertado, em via impressa devidamente preenchida e assinada, junto à documentação de habilitação, observadas as condições dos itens abaixo.

2.2. ATENÇÃO: os valores finais ofertados serão determinados mediante a utilização do arquivo XLSX disponível pelo endereço https://tinyurl.com/4jrfhbve , no qual:

a) os valores unitários relativos ao global negociado com o pregoeiro advirão da aplicação linear, sobre os correspondentes valores unitários originalmente ofertados, do desconto em relação ao valor global originalmente ofertado a que corresponde o valor global negociado;

b) os valores finais mensais e unitários serão os obtidos conforme a alínea anterior truncados na segunda casa decimal.

2.2.1. Nos preços readequados permanecerão incluídos todos os impostos, tributos, encargos, custos e/ou quaisquer outros ônus que porventura possam recair sobre a prestação do objeto da licitação, os quais ficarão a cargo única e exclusivamente do licitante contratado.

2.2.2. Quaisquer custos diretos ou indiretos omitidos da proposta comercial ou incorretamente cotados serão considerados inclusos no preço, não sendo admitidos pleitos de acréscimo a esse ou a qualquer título, devendo o objeto licitado ser prestado sem qualquer ônus adicional para o BDMG.

2.3. ATENÇÃO: a não aceitação, pelo licitante, das condições a que se refere o item 2.2 deste anexo implicará na desclassificação da proposta.

2.4. A proposta comercial será assinada pelo licitante ou seu representante legal, ou ainda por procurador devidamente constituído, sem emendas, acréscimos, borrões, rasuras, ressalvas, entrelinhas ou omissões, no teor do modelo abaixo indicado:

PREGÃO ELETRÔNICO BDMG-19/2026	
1. NOME EMPRESARIAL: *<nome da licitante>*	
2. ENDEREÇO: <endereço completo>	
3. CNPJ: <nº do CNPJ>	
4. TELEFONE: <nº do telefone>	**5. E-MAIL:** <endereço de e-mail>

6. OBJETO: Contratação de empresa especializada na prestação de serviços gerenciados de Centro de Operações de Segurança (SOC), em regime de operação contínua 24x7x365.

7. VALOR PROPOSTO:

Item	Descrição	Unidade	Quantidade total	Valor mensal/unitário	Valor anual
1	Serviço Gerenciado de Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR)	Serviço Mensal	12 (doze)	R$ <preencher>	R$ <preencher>
2	Serviço de Gestão de Vulnerabilidades	Serviço Mensal	12 (doze)	R$ <preencher>	R$ <preencher>
3	Licenças de uso de solução de Gestão de Vulnerabilidades com Gerenciamento de Patches, por 12 (doze) meses	Ativos monitorados	1.200 (mil e duzentos)	R$ <preencher>	R$ <preencher>
TOTAL					R$ <preencher>

VALOR GLOBAL PROPOSTO: R$ <valor> (<valor por extenso>)

8. DECLARAÇÕES:

Declaro que conheço, aceito e serão atendidas todas as condições estabelecidas no Pregão Eletrônico BDMG-19/2026 e seus anexos.

Declaro que o preço proposto engloba todos os custos, diretos e indiretos, e ônus decorrentes da prestação dos serviços, tais como tributos, contribuições fiscais e parafiscais, encargos trabalhistas e previdenciários, taxas, fretes, insumos, custos operacionais, ou outros necessários ao cumprimento integral do objeto do instrumento contratual ou ainda quaisquer outros que porventura possam recair o referido instrumento, não cabendo ao BDMG quaisquer custos adicionais.

Declaro que esta proposta foi elaborada de forma independente.

Declaro, que inexistem fatos impeditivos à contratação pelo BDMG, prescritos na legislação específica, inclusive os previstos no artigo 11 do Regulamento de Licitações e Contratos do BDMG.

Declaro, sob as penas da lei, que em nenhuma das dependências deste proponente ocorre trabalho noturno, perigoso ou insalubre por menores de 18 (dezoito) anos ou qualquer trabalho por menores de 16 (dezesseis) anos, salvo na condição de aprendiz, na forma da Lei.

Autorizo a coleta e o tratamento, pelo BDMG, dos dados pessoais fornecidos neste instrumento de proposta e nos demais documentos entregues para participação nesta licitação, para as finalidades

constantes do Edital em referência e seus efeitos, conforme disposições da Política de Privacidade e Proteção de Dados Pessoais do BDMG e da legislação aplicável.
9. PRAZO DE VALIDADE DA PROPOSTA: <*escrever n° de dias*> (<*escrever por extenso n° de dias*>) dias corridos contados da data de apresentação deste instrumento de proposta ao BDMG **Observação**: mínimo de 60 (sessenta) dias corridos.
10. DATA E ASSINATURA <local>, <dia> de <mês> de 2026. _____ ***<escrever nome do representante legal que assina a proposta>*** ***<escrever n° de CPF do representante legal que assina a proposta>***

2.5. Caso não conste detalhado no instrumento de proposta, assumir-se-á ofertado o prazo de 60 (sessenta) dias para a validade da proposta, contados da apresentação do instrumento de proposta ao BDMG.

2.6. O instrumento impresso da proposta assinada por procurador será enviado acompanhado do original ou cópia autenticada do instrumento de procuração devidamente assinado, observadas as seguintes condições:

2.6.1. A procuração apresentada será por instrumento público ou particular, com firma reconhecida em cartório, na qual o licitante, na pessoa de seu(s) competente(s) representante(s) legal(is), outorgue expressos poderes para atuar no âmbito do pregão e praticar todos os atos pertinentes ao certame em nome do licitante.

2.6.2. No caso de licitante pessoa jurídica, a procuração por instrumento particular será entregue acompanhada do respectivo contrato ou estatuto social, consolidado ou acompanhado das alterações em vigor, e ainda, no caso de ser a procuração outorgada por representante(s) legal(is) eleito(s) em ato apartado, cópia autenticada da ata de reunião ou assembleia em que se deu a eleição do(s) outorgante(s).

2.6.3. No caso de substabelecimento, será apresentado junto ao instrumento próprio cópia autenticada da procuração concedida pelo licitante ao substabelecente e o substabelecimento terá a(s) firma(s) do(s) outorgante(s) reconhecida(s) em cartório.

2.6.3.1. Não se admitirá substabelecimento caso proibido no instrumento de procuração, ressalvada a hipótese de ratificação expressa do próprio licitante, que retroagirá à data do ato.

2.7. Alternativamente, o instrumento de proposta comercial readequada ao último valor ofertado poderá ser apresentado em via digital assinada mediante certificação digital, desde que comprovada pelo Pregoeiro a autenticidade da(s) firma(s) eletrônica(s) e desde que, conforme o caso, a

autenticidade e validade da documentação a que se refere o item 2.6 *supra* e respectivos subitens seja também aferida mediante consulta aos respectivos sítios da internet.

ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL

CONTRATO DE PRESTAÇÃO DE SERVIÇOS CELEBRADO ENTRE O BANCO DE DESENVOLVIMENTO DE MINAS GERAIS S/A. - BDMG E <NOME DA CONTRATADA>

BANCO DE DESENVOLVIMENTO DE MINAS GERAIS S/A. - BDMG, CNPJ nº 38.486.817/0001-94, com sede em Belo Horizonte/MG, na Rua da Bahia, nº 1600 – Bairro de Lourdes, CEP: 30.160-907, a seguir denominado BDMG, e <NOME EMPRESARIAL DA CONTRATADA>, CNPJ nº <Nº DO CNPJ>, estabelecida em <ENDEREÇO COMPLETO>, a seguir denominada CONTRATADA, resolvem, por seus representantes legais ao final assinados, celebrar o presente contrato, objeto da licitação **EDITAL BDMG-19/2026**, homologada pela autoridade competente do BDMG em <DATA DA HOMOLOGAÇÃO>, conforme publicado no "Minas Gerais" de <DATA DE PUBLICAÇÃO DA HOMOLOGAÇÃO>, mediante as cláusulas e condições seguintes.

CLÁUSULA 1 - REGÊNCIA NORMATIVA

1.1. Aplicam-se ao presente contrato a Lei Federal nº 13.303/2016; Lei Estadual nº 13.994/2001; Decreto Estadual nº 45.902/2012; Decreto Estadual nº 47.154/2017; o Regulamento de Licitações e Contratos do BDMG, os normativos e legislação específicos e a legislação supletiva, no que couber.

1.2. Aplicam-se também a esta contratação, independentemente de anexação ou transcrição, o EDITAL BDMG-19/2026, com todos os seus anexos e apêndices, a ata da sessão pública e a proposta da CONTRATADA, datada de XX de XXXXXX de 20XX.

CLÁUSULA 2 - OBJETO

2.1. Constitui objeto deste contrato a prestação de serviços gerenciados de Centro de Operações de Segurança (SOC), em regime de operação contínua 24x7x365 (24 horas por dia, 7 dias por semana, 365 dias por ano), compreendendo:

(i) Serviço Gerenciado de Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR), que abrange o monitoramento e a detecção de ameaças, a Inteligência de Ameaças (Threat Intelligence), executada por equipe própria e distinta, na forma do item 3.7 do Anexo IV-A – Termo de Referência – Requisitos, a Caça a Ameaças Cibernéticas (Threat Hunting), executada em regime contínuo e integrado à operação do SOC, sem franquia de horas técnicas e sem requisição de serviço prévia para as campanhas programadas, na forma do item 3.4 do Anexo IV-A – Termo de Referência – Requisitos, a Engenharia de Detecção e Otimização do SIEM, executada sobre a plataforma Microsoft Sentinel de propriedade do BDMG, e a Resposta a Incidentes;

(ii) Serviço de Gestão de Vulnerabilidades; e

(iii) Licenças de uso de solução de Gestão de Vulnerabilidades com Gerenciamento de Patches, por 12 (doze) meses, para 1.200 (mil e duzentos) ativos monitorados, na forma do Anexo IV-A – Termo de Referência – Requisitos.

INFORMAÇÃO CONTROLADA

2.2. Os serviços são de natureza continuada e serão executados, medidos e faturados mensalmente, em 12 (doze) parcelas por período contratual de operação, ressalvado o último período contratual, de 10 (dez) parcelas, conforme medição atestada pela fiscalização, observados o modelo de execução, o modelo de gestão e os critérios de medição, níveis mínimos de serviço, indicadores de desempenho e glosas previstos nos itens 11 (Forma e Condições de Execução do Objeto), 11.15 a 11.18 (governança e reuniões de acompanhamento) e 12 (Acordo de Níveis de Serviço) do Anexo IV-A – Termo de Referência – Requisitos.

2.3. O licenciamento, bem como os custos de ingestão, retenção e automação da plataforma de Microsoft Sentinel serão de responsabilidade do BDMG. Compete à CONTRATADA exclusivamente a administração, operação, sustentação, engenharia de detecção e automação da plataforma no ambiente do BDMG.

2.4. É vedado à CONTRATADA ofertar, precificar ou impor o fornecimento de plataforma de SIEM e/ou de SOAR, ou de qualquer ferramenta que duplique as funções nativas do Microsoft Sentinel, não podendo eventual ferramenta acessória de seu uso interno constituir condição para a prestação do serviço, tampouco receptáculo exclusivo de dados, regras, casos ou evidências do BDMG. Ressalvam-se dessa vedação a ferramenta de ITSM de que trata o subitem 3.5 e, quando adotada a alternativa do subitem 9.1 do Anexo IV-A – Termo de Referência – Requisitos, o portal da própria CONTRATADA, cujo fornecimento constitui obrigação da CONTRATADA e integra o objeto, sem que os registros e dados neles mantidos configurem receptáculo exclusivo, por serem de propriedade do BDMG e por ele integralmente acessíveis e exportáveis, na forma dos subitens 3.5.1 a 3.5.3 deste contrato e dos subitens 9.6 e 9.10 do Anexo IV-A – Termo de Referência – Requisitos.

2.5. A execução do objeto vincula-se integralmente ao Anexo IV-A – Termo de Referência – Requisitos, que integra este contrato, bem como à proposta da CONTRATADA, prevalecendo, em caso de divergência, as disposições do edital e de seus anexos.

2.6. Atividades que necessitem ou representem risco de interrupção de serviços do ambiente computacional do BDMG serão agendadas previamente e realizadas fora do horário de funcionamento do Banco, que ocorre nos dias úteis das 8h às 20h, salvo quando expressamente autorizadas.

2.7. Atividades realizadas pela CONTRATADA fora do horário de funcionamento do BDMG, ou em finais de semana e feriados, não ensejarão qualquer pagamento adicional por parte do BDMG.

CLÁUSULA 3 - FORMA E CONDIÇÕES DE EXECUÇÃO DO OBJETO

3.1. A prestação dos serviços terá início na data de assinatura do contrato e compreende dois escopos sucessivos e distintos: o escopo de IMPLANTAÇÃO, na forma dos subitens 3.3 a 3.3-B deste contrato e dos subitens 11.1 a 11.11 do Anexo IV-A – Termo de Referência – Requisitos, e o escopo de OPERAÇÃO, correspondente à prestação plena dos serviços continuados a partir da emissão do Termo de Recebimento Definitivo (TRD) e pelo prazo de vigência contratual, na forma dos subitens 11.12 a 11.18 do Anexo IV-A – Termo de Referência – Requisitos.

INFORMAÇÃO CONTROLADA

3.2. O BDMG disponibilizará à CONTRATADA os acessos nominais ao ambiente Microsoft Sentinel do Banco em até 10 (dez) dias úteis contados da data de assinatura do contrato, limitados a 10 (dez) contas nominais ativas simultâneas.

3.2.1. Os acessos serão nominais e individualizados, vedados o compartilhamento de credenciais e a utilização de contas genéricas, e serão concedidos exclusivamente aos profissionais formalmente designados pela CONTRATADA para a execução deste contrato, observadas as modalidades, os controles e as vedações estabelecidos nesta CLÁUSULA e no item 7.15.10 do Anexo IV-A – Termo de Referência – Requisitos.

3.2.2. A concessão de acessos em quantidade superior ao limite previsto no subitem 3.2 dependerá de justificativa técnica formal da CONTRATADA e de autorização prévia e expressa da Superintendência de Tecnologia da Informação do BDMG, não gerando ao Banco qualquer obrigação de deferimento nem à CONTRATADA direito a reequilíbrio ou a pagamento adicional.

3.2.3. Os acessos concedidos serão objeto de revisão trimestral formal, com revogação, em até 5 (cinco) dias úteis, dos acessos não utilizados no período, dos excedentes ao necessário e dos titulares desligados ou remanejados, mediante evidência formal apresentada ao BDMG.

3.3. A implantação inicial será formalizada por Plano de Implantação e por Termo de Recebimento Definitivo (TRD), a ser concluída no prazo de até 60 (sessenta) dias corridos contados da assinatura do contrato, correspondentes aos até 2 (dois) meses do escopo de IMPLANTAÇÃO de que tratam o subitem 5.1 deste contrato e o subitem 1.1.1 do Anexo IV-A – Termo de Referência – Requisitos.

3.3-A. O Plano de Implantação contemplará, obrigatoriamente e de forma segregada, as duas frentes do objeto: (i) SOC/MDR e Microsoft Sentinel; e (ii) Gestão de Vulnerabilidades e Patch Management, com cronograma, marcos, responsáveis, dependências e evidências próprios para cada frente, submetendo-se ambas, integralmente, aos critérios de aceite do item 11.11 do Anexo IV-A – Termo de Referência – Requisitos.

3.3-B. A frente de Gestão de Vulnerabilidades e Patch Management compreenderá, no mínimo: a ativação da solução com licenças válidas para 1.200 (mil e duzentos) ativos monitorados; a descoberta e o inventário dos ativos do escopo, conciliados com o inventário do BDMG; a execução do primeiro ciclo completo de varredura autenticada da rede interna, do primeiro ciclo de varredura dos ativos expostos à internet e do primeiro ciclo de análise dinâmica (DAST) dos FQDNs definidos pelo BDMG; a integração ao Microsoft Sentinel do BDMG e ao Portal de Visibilidade Executiva e Operacional, na forma do subitem 9.17 do Anexo IV-A – Termo de Referência – Requisitos; a configuração e a homologação do patch management com anéis de implantação, grupos piloto, janelas de manutenção, blackout windows, regras de aprovação, rollback e exceções; a aprovação, pelo BDMG, da lista de ativos críticos e não críticos; a entrega do Relatório Inicial de Exposição; e a capacitação inicial das equipes do Banco, tudo na forma dos itens 4 e 5 e da alínea 'd' do item 11.11 do Anexo IV-A – Termo de Referência – Requisitos.

3.3-C. O prazo de conclusão da frente de que trata o subitem 3.3-B é o mesmo previsto no subitem 3.3 e conta-se igualmente da assinatura do contrato. O atraso do BDMG na disponibilização dos acessos de que trata o subitem 3.2, bem como qualquer outra pendência de sua responsabilidade, resolve-se exclusivamente pela suspensão de prazo do subitem 3.3.1, não deslocando o termo inicial de contagem.

3.3.1. O prazo previsto no subitem 3.3 ficará suspenso pelo período em que a execução depender de providência formalmente registrada como pendência de responsabilidade do BDMG na ferramenta de ITSM de que trata o subitem 3.5, retomando-se a contagem a partir do respectivo atendimento. A suspensão somente produz efeito a partir do registro e da comunicação simultânea ao BDMG, cabendo à CONTRATADA o ônus de comprovar a pendência invocada.

3.3.2. Durante a implantação e até a emissão do TRD, os serviços de monitoramento serão prestados em regime de operação assistida, sem remuneração e sem aplicação de glosas, com medição e reporte dos indicadores contratuais para fins de acompanhamento, observado o subitem 4.4.

3.3.3. Concluídas as atividades previstas no subitem 3.3, a CONTRATADA deverá comunicar formalmente o fato à Superintendência de Tecnologia da Informação do BDMG, apresentando toda a documentação, evidências e informações necessárias à verificação do atendimento das condições contratuais, incluindo, quando aplicável, o Plano de Implantação concluído, as evidências de ativação e configuração do ambiente e as credenciais de acesso ao ambiente provisionado.

3.4. A execução se dará em modelo híbrido, com monitoração e resposta a incidentes predominantemente remotas, plantão contínuo 24x7x365 para incidentes de segurança da informação e alocação de profissional dedicado/N3 em regime híbrido, com trabalho presencial na sede do BDMG, em Belo Horizonte/MG, em 3 (três) dias por semana, em dias úteis e no horário comercial do Banco, segundo agenda previamente acordada com a fiscalização do contrato, e com presença física adicional sempre que convocado, na forma dos itens 7.15, 7.15.4 e 7.15.8 do Anexo IV-A – Termo de Referência – Requisitos.

3.4.1. As despesas de deslocamento, transporte, hospedagem e alimentação decorrentes do trabalho presencial e das convocações extraordinárias correm por conta exclusiva da CONTRATADA e consideram-se incluídas no preço proposto.

3.5. Todas as demandas, chamados, evidências e registros de tempo serão lançados na ferramenta de ITSM disponibilizada pela CONTRATADA, sem custo adicional para o BDMG, a qual constitui o sistema de registro oficial para apuração de SLA, glosas e medição, prevalecendo seus registros em qualquer divergência. O BDMG não dispõe de ferramenta própria de ITSM, competindo à CONTRATADA fornecê-la, implantá-la, operá-la, sustentá-la e mantê-la licenciada durante toda a vigência contratual.

3.5.1. A CONTRATADA assegurará ao BDMG acesso nominal, individualizado, irrestrito e em tempo real à ferramenta de ITSM, para as equipes de gestão contratual, fiscalização, tecnologia da informação, segurança da informação e auditoria interna do Banco, sem custo adicional e sem limitação de perfil, de campos ou de período de consulta, bem como a exportação integral dos chamados, classificações, históricos de tramitação, anexos, evidências e carimbos de tempo,

em CSV e JSON, a qualquer tempo, por interface própria e por API, independentemente de solicitação, intermediação ou autorização prévia.

3.5.2. Os chamados, as classificações, os históricos de tramitação, os registros de tempo, os anexos e as evidências produzidos na ferramenta de ITSM em razão deste contrato são de propriedade exclusiva do BDMG, ainda que hospedados em ambiente da CONTRATADA, que atua na condição de mera operadora e custodiante, vedadas a remoção, a supressão, a alteração retroativa, a ofuscação, a criptografia com chave exclusiva da CONTRATADA e o condicionamento do acesso a qualquer pagamento adicional, aplicando-se-lhes as obrigações da CLÁUSULA 10 – CONFIDENCIALIDADE. A ferramenta manterá trilha de auditoria imutável das alterações de status, de classificação e de carimbos de tempo, com identificação de autor, data e hora, acessível ao BDMG.

3.5.3. Ao término da vigência, na rescisão ou na hipótese de não renovação, a CONTRATADA entregará ao BDMG, no prazo de até 10 (dez) dias úteis contados do início da transição de que trata o subitem 3.8, a base integral dos registros referidos no subitem 3.5.2, em formatos abertos (CSV e JSON) e com dicionário de dados, sem custo adicional, procedendo à eliminação das cópias remanescentes em seu ambiente somente após a confirmação formal, pelo BDMG, do recebimento íntegro e legível da base, ressalvadas as obrigações legais de retenção. A indisponibilidade, a falha ou a limitação da ferramenta de ITSM não suspende os prazos dos níveis mínimos de serviço, não enseja suspensão de contagem e não constitui excludente de glosa, devendo a CONTRATADA manter procedimento formal de registro contingencial e promover, em até 1 (um) dia útil do restabelecimento, o lançamento retroativo dos chamados com os respectivos horários reais.

3.6. A CONTRATADA manterá, durante toda a vigência contratual e sem custo adicional, os canais de atendimento para acionamento e abertura de chamados previstos nos itens 8.6 e 8.7 do Anexo IV-A – Termo de Referência – Requisitos, compreendendo, no mínimo, portal de ITSM próprio acessível via internet, telefone gratuito nacional (0800) com atendimento humano, WhatsApp corporativo em número institucional e correio eletrônico institucional de atendimento, todos em regime 24x7x365 para incidentes de segurança da informação. Os respectivos números, endereços e procedimentos de acionamento serão informados formalmente ao BDMG na etapa de implantação, constituem condição para a emissão do Termo de Recebimento Definitivo e somente poderão ser alterados mediante comunicação prévia ao Banco, com antecedência mínima de 15 (quinze) dias corridos. A indisponibilidade dos canais não suspende nem prorroga os prazos contratuais e sujeita a CONTRATADA às glosas do item 12.25 do Anexo IV-A – Termo de Referência – Requisitos.

3.7. A CONTRATADA versionará todo o conteúdo produzido na execução contratual, em especial regras analíticas, consultas KQL, parsers, funções, playbooks, automation rules, workbooks, watchlists e hunting queries, em repositório Git indicado pelo BDMG, em formatos abertos, com revisão, testes e procedimento de rollback documentado.

3.7.1. A CONTRATADA poderá empregar recursos de Inteligência Artificial Generativa como apoio à triagem, ao enriquecimento e à sumarização de eventos e incidentes, observado o item 3.8 do Anexo IV-A – Termo de Referência – Requisitos, sendo obrigatória a validação humana prévia por profissional qualificado (human-in-the-loop) antes da execução de qualquer ação em

ambiente de produção do Banco, vedada a execução automática ou não supervisionada e vedada a utilização de dados do BDMG para treinamento, ajuste fino ou aperfeiçoamento de modelos, na forma da alínea 'a' do subitem 9.4 deste contrato.

3.8. Ao término da vigência, na rescisão ou na hipótese de não renovação, a CONTRATADA executará transição assistida pelo período de até 60 (sessenta) dias, prorrogável uma vez por igual período a critério do BDMG, mantidas as condições contratuais e a remuneração proporcional, com handover técnico assistido, entrega da documentação As-Built e transferência de conhecimento.

3.9. Encerrada a transição, a CONTRATADA revogará, em até 5 (cinco) dias úteis, todos os acessos nominais, contas convidadas, delegações, chaves de API e contas de serviço, apresentando ao BDMG evidência formal da revogação e da eliminação de cópias de dados do Banco em seu ambiente, ressalvadas as obrigações legais de retenção.

CLÁUSULA 4 - RECEBIMENTO DO OBJETO

4.1. Unidade responsável pelo recebimento: Superintendência de Tecnologia da Informação.

4.2. Será dado ACEITE PROVISÓRIO da etapa de implantação mediante a comunicação, pela CONTRATADA, da conclusão do Plano de Implantação de que trata o subitem 3.3.3.

4.3. Recebida a comunicação de que trata o subitem 3.3.3, o BDMG terá até 15 (quinze) dias corridos para verificar o atendimento dos critérios de aceite do subitem 11.11 do Anexo IV-A – Termo de Referência – Requisitos e manifestar-se formalmente pelo aceite ou pela rejeição, total ou parcial, com a indicação das não conformidades identificadas.

4.3.1. Na hipótese de rejeição, a CONTRATADA promoverá as correções, complementações ou ajustes necessários no prazo máximo de 5 (cinco) dias corridos, sem ônus adicional para o BDMG, e a entrega será novamente submetida à verificação de que trata o subitem 4.3, cujo prazo será contado do recebimento das correções.

4.3.2. O ACEITE DEFINITIVO da etapa de implantação será formalizado pela emissão do Termo de Recebimento Definitivo (TRD), que somente poderá ocorrer após a homologação formal, pelo BDMG, de todos os critérios de aceite do subitem 11.11 do Anexo IV-A – Termo de Referência – Requisitos, não se aplicando à etapa de implantação a presunção de aceite do subitem 4.8.

4.4. A emissão do TRD marca o início do escopo de OPERAÇÃO, a partir do qual será permitido o faturamento, na forma da CLÁUSULA 7 – PAGAMENTO, não sendo devido à CONTRATADA nenhum pagamento antes dela.

4.5. Os serviços continuados serão recebidos mensalmente mediante a apresentação, pela CONTRATADA, até o 5º (quinto) dia útil do mês subsequente ao de referência, do relatório gerencial previsto no item 11.13 do Anexo IV-A – Termo de Referência – Requisitos, acompanhado obrigatoriamente dos dados brutos que o sustentam em CSV e JSON, e da respectiva medição, a ser atestada pela fiscalização com a apuração das glosas do item 12.25 do mesmo anexo.

INFORMAÇÃO CONTROLADA

4.6. O BDMG dará ACEITE DEFINITIVO da medição mensal no prazo de 5 (cinco) dias úteis contados da apresentação dos documentos de que trata o subitem 4.5 ou, se for o caso, do recebimento, pelo Banco, de correções ou adequações.

4.7. Caso seja detectada alguma divergência entre os serviços prestados e o objeto contratado, ou entre a medição apresentada e os registros da ferramenta de ITSM de que trata o subitem 3.5, apurados pelo BDMG a partir dos dados brutos exportados na forma do subitem 3.5.1, será emitido um aviso para que a CONTRATADA proceda, no prazo de 5 (cinco) dias úteis, com as devidas correções e posterior comunicação ao BDMG.

4.8. Na hipótese de o ACEITE DEFINITIVO da medição mensal não ser efetivamente emitido dentro do prazo fixado no subitem 4.6, reputar-se-á a medição definitivamente aceita, desde que inexista qualquer manifestação em contrário do BDMG.

4.9. Somente após o ACEITE DEFINITIVO, ou da sua presunção, a CONTRATADA poderá emitir e encaminhar o devido documento fiscal ou equivalente, no valor da medição atestada, líquido das glosas apuradas no período de referência.

CLÁUSULA 5 - VIGÊNCIA E PRORROGAÇÃO

5.1. O contrato terá vigência de 14 (quatorze) meses, contados da data de sua assinatura, compreendendo dois escopos sucessivos: (i) o escopo de IMPLANTAÇÃO, de até 2 (dois) meses, encerrado pela emissão do Termo de Recebimento Definitivo (TRD); e (ii) o escopo de OPERAÇÃO, de 12 (doze) meses de prestação continuada dos serviços, contados da emissão do TRD.

5.1.1. Concluída a implantação em prazo inferior a 2 (dois) meses, a diferença não será remunerada e a vigência contratual se encerrará com o decurso do 12º (décimo segundo) mês de operação, podendo, nessa hipótese, ser inferior a 14 (quatorze) meses.

5.1.2. O atraso na emissão do TRD imputável à CONTRATADA não prorroga a vigência contratual nem gera direito à remuneração dos meses de operação não prestados, sujeitando-a às sanções da CLÁUSULA 16 e às glosas do subitem 12.25 do Anexo IV-A – Termo de Referência – Requisitos. O atraso decorrente de fato imputável ao BDMG, de caso fortuito ou de força maior, apurado na forma do subitem 11.7 do mesmo anexo, será compensado mediante termo aditivo, sem alteração do número de parcelas mensais do escopo de OPERAÇÃO.

5.2. O contrato poderá ser prorrogado sucessivamente, mediante termo aditivo, por interesse das partes, alcançando a prorrogação exclusivamente o escopo de OPERAÇÃO, e observado o limite máximo de 5 (cinco) anos contados da celebração do contrato, na forma do art. 71 da Lei Federal nº 13.303, de 30 de junho de 2016.

5.2.1. Cada prorrogação terá duração de 12 (doze) meses de operação, ressalvado o último período contratual, que terá duração de 10 (dez) meses, de modo que a soma dos períodos — até 2 (dois) meses de implantação e 12 (doze) meses de operação no período inicial, 12 (doze) meses de operação em cada um dos três períodos prorrogados seguintes e 10 (dez) meses de operação no último — não exceda 60 (sessenta) meses contados da celebração do contrato.

INFORMAÇÃO CONTROLADA

5.2.2. O escopo de IMPLANTAÇÃO não se renova nem se repete nas prorrogações, não havendo, em nenhuma delas, nova mobilização remunerada, novo Plano de Implantação, novo Termo de Recebimento Definitivo ou qualquer parcela a título de implantação, integração, ativação ou capacitação inicial. Também não se renova a estabilização escalonada das glosas prevista no subitem 12.11 do Anexo IV-A – Termo de Referência – Requisitos, concedida uma única vez.

5.2.3. A prorrogação não é automática nem constitui direito subjetivo da CONTRATADA, dependendo de interesse das partes e ficando condicionada à demonstração de vantajosidade, à manutenção das condições de habilitação, ao interesse institucional do BDMG e à avaliação satisfatória do desempenho no período, aferida pelos indicadores do item 12 do Anexo IV-A – Termo de Referência – Requisitos.

5.2.4. Na hipótese de extinção antecipada, a vigência se encerrará na data indicada no ato de extinção, assegurada, em qualquer caso, a execução integral da transição assistida prevista no subitem 3.8 deste contrato e no subitem 14.3 do Anexo IV-A – Termo de Referência – Requisitos.

5.3. Este contrato poderá ser alterado, por acordo entre as partes, nos termos da Lei Federal 13.303/2016 e do Regulamento de Licitações e Contratos do BDMG.

CLÁUSULA 6 - VALOR, REAJUSTE E DOTAÇÃO ORÇAMENTÁRIA

6.1. O valor da presente contratação será de R$ XXXXXX (XXXXXXXXXXXXXXXXXXXXX).

6.1.1. O valor referido no subitem 6.1 corresponde ao primeiro período contratual, de 14 (quatorze) meses, e remunera exclusivamente o escopo de OPERAÇÃO, em 12 (doze) parcelas mensais fixas, e o licenciamento de que trata o item 3 do quadro de itens do subitem 1.1 do Anexo IV-A – Termo de Referência – Requisitos, em parcela única. Não há, no valor contratado, parcela específica de remuneração do escopo de IMPLANTAÇÃO, cujos custos se consideram integralmente diluídos nas parcelas mensais de operação.

6.2. Os recursos para esta contratação encontram-se na conta orçamentária nº 8173900047 SERVIÇOS DE SEGURANÇA - TI para o exercício de 2026 nas contas correspondentes para os exercícios subsequentes.

6.3. Decorridos 12 (doze) meses da data de apresentação da proposta ou do último reajuste ocorrido, os preços pactuados serão reajustados pelo Índice Nacional de Preços ao Consumidor Amplo – IPCA, divulgado pelo Instituto Brasileiro de Geografia e Estatística – IBGE, ou por outro índice que vier a substituí-lo.

6.4. O índice a ser aplicado corresponderá à variação acumulada dos índices efetivamente publicados nos 12 (doze) meses do período de referência, passando os valores reajustados a ser exigíveis a partir do primeiro dia do período mensal seguinte àquele em que se der a exigibilidade do reajuste.

6.5. Somente será devido reajuste para as parcelas que ainda não tenham sido quitadas até a data de exigibilidade do reajuste.

CLÁUSULA 7 - PAGAMENTO

INFORMAÇÃO CONTROLADA

7.1. Os valores correspondentes aos itens 1 e 2 do quadro de itens do subitem 1.1 do Anexo IV-A – Termo de Referência – Requisitos — Serviço Gerenciado de Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR) e Serviço de Gestão de Vulnerabilidades — serão pagos em parcelas mensais fixas, a partir da emissão do Termo de Recebimento Definitivo (TRD), após o aceite definitivo da medição mensal e do Relatório Mensal de Aferição dos Níveis Mínimos de Serviço, na forma da CLÁUSULA 4, deduzidas as glosas apuradas no período.

7.1.1. Não é devido pagamento a título do escopo de IMPLANTAÇÃO, que não constitui item remunerável desta contratação. Os custos de mobilização, integração de fontes, desenvolvimento de parsers e de casos de uso, implantação e homologação das ferramentas, projeto executivo, capacitação inicial e demais atividades desse escopo consideram-se integralmente diluídos nas parcelas mensais do escopo de OPERAÇÃO, sendo vedada a apresentação de documento fiscal a esse título.

7.1.2. Nenhum pagamento será devido à CONTRATADA antes da emissão do TRD, que marca o início do escopo de OPERAÇÃO e da remuneração mensal.

7.1.3. O valor correspondente ao item 3 do quadro de itens — licenças de uso da solução de Gestão de Vulnerabilidades com Gerenciamento de Patches — será pago em parcela única, após a emissão do TRD e, nas prorrogações, após a formalização do respectivo termo aditivo, correspondendo o licenciamento a cada período contratual de operação: 12 (doze) meses nos quatro primeiros períodos e 10 (dez) meses no último.

7.1.4. Nas prorrogações não se repete a etapa de implantação e não é devida remuneração a título de implantação, mobilização ou capacitação inicial, na forma do subitem 5.2.2.

7.2. O **BDMG** realizará o pagamento em até 10 (dez) dias úteis contados da data de apresentação do documento fiscal, mediante crédito em conta corrente de titularidade da **CONTRATADA**, ou outra forma legalmente admitida.

7.3. O documento fiscal deverá ser entregue ao **BDMG** pela **CONTRATADA**, no prazo de até 05 (cinco) dias úteis contados da data do recebimento definitivo correspondente, ou da sua presunção, devendo a entrega ser realizada até o dia 24 (vinte e quatro) do mês da emissão do respectivo documento fiscal, ou anteriormente ao antepenúltimo dia útil, quando a data de pagamento for no mês subsequente à sua emissão.

7.3.1. Caso os prazos para entrega do documento fiscal não sejam observados, o **BDMG** poderá exigir a sua troca.

7.4. Não será efetuado pagamento contra a apresentação de documento sem valor fiscal, a não ser que a **CONTRATADA** esteja desobrigada de apresentá-lo, condição que deverá comprovar, mediante indicação da legislação específica, quando da assinatura do contrato.

7.5. O documento fiscal deverá ser emitido em nome do Banco de Desenvolvimento de Minas Gerais S.A. – **BDMG**, CNPJ nº 38.486.817/0001-94, e nele deverão constar os dados do instrumento contratual firmado bem como os dados do banco, agência e conta corrente da **CONTRATADA** para a efetivação do pagamento, se esta for a opção.

INFORMAÇÃO CONTROLADA

7.6. O eventual atraso na entrega do documento fiscal acarretará correspondente e proporcional atraso no pagamento, sem qualquer penalização ou atualização monetária.

7.7. Caso seja constatada qualquer irregularidade no documento fiscal emitido pela **CONTRATADA**, aquele será devolvido para correção, sendo restabelecido o prazo de 05 (cinco) dias úteis para pagamento, a contar do recebimento pelo **BDMG** do documento corrigido.

7.8. Estarão incluídos no valor contratado todos os custos, diretos e indiretos, e ônus decorrentes do fornecimento, tais como tributos, contribuições fiscais e parafiscais, encargos, inclusive trabalhistas, taxas, fretes, insumos e custos operacionais, bem como quaisquer outras despesas necessárias à execução do contrato, e correrão por conta da **CONTRATADA**, não cabendo ao **BDMG** quaisquer custos adicionais.

7.9. A **CONTRATADA** é responsável por todos os tributos e contribuições federais, estaduais e municipais devidos em decorrência do objeto contratado, inclusive aqueles retidos pelo **BDMG** na forma da lei, devendo destacar as retenções tributárias devidas no documento fiscal apresentado ou entregar documentação comprobatória que comprove a necessidade de não retenção de certo(s) tributo(s).

7.10. Ocorrendo atraso injustificado de pagamento por parte do **BDMG**, o valor será atualizado financeiramente pela aplicação do índice utilizado para cálculo do rendimento da poupança no mês anterior à data prevista para pagamento, proporcional aos dias em atraso.

7.11. Em nenhuma hipótese ocorrerá a antecipação do pagamento para viabilizar o cumprimento do objeto contratado.

7.12. Na hipótese de o dia de pagamento cair em feriado bancário, considerar-se-á prorrogado o prazo até o dia útil seguinte (art. 132, § 1º – C.C.).

CLÁUSULA 8 - ENCARGOS DAS PARTES

8.1. São obrigações do **BDMG**:

a) prestar à **CONTRATADA** esclarecimentos e informações sobre desajustes ou problemas detectados na execução do contrato, exigindo que sejam tomadas todas as providências necessárias ao seu bom andamento;

b) zelar pela adequada execução do contrato, em especial quanto ao acompanhamento e fiscalização do serviço, à exigência de condições estabelecidas e à aplicação de sanções;

c) rejeitar, no todo ou em parte, o objeto entregue pela **CONTRATADA** fora das especificações fixadas no contrato;

d) efetuar o pagamento de acordo com as condições contratadas;

e) fornecer à CONTRATADA cópia da Política de Segurança da Informação e Cibernética do BDMG e das demais normas internas aplicáveis à execução do objeto, bem como comunicar as respectivas atualizações;

f) proporcionar as informações, os acessos e as facilidades necessários para que a CONTRATADA possa cumprir suas obrigações nos prazos e nas condições contratados, observado o disposto no subitem 3.2;

INFORMAÇÃO CONTROLADA

g) rejeitar, de forma justificada, no todo ou em parte, os serviços executados em desacordo com as especificações, e solicitar à CONTRATADA e a seus prepostos as providências necessárias ao bom andamento dos serviços;

h) exercer as competências de gestão que lhe são próprias, em especial a definição e a validação do serviço de negócio e da criticidade de cada ativo, a aprovação da Lista de Ativos Críticos referida no item 12.8 do Anexo IV-A – Termo de Referência – Requisitos e de suas atualizações, a decisão sobre o regime de contenção aplicável a cada ativo e a deliberação sobre as ações de alto impacto;

i) registrar na ferramenta de ITSM as pendências e as providências sob sua responsabilidade, de modo a permitir a apuração objetiva das hipóteses de suspensão de prazo previstas nos itens 12.8, 12.9 e 12.10 do Anexo IV-A – Termo de Referência – Requisitos.

8.2. São obrigações da **CONTRATADA**:

a) realizar o objeto contratado conforme todos as condições fixadas nos termos acordados no instrumento contratual;

b) reparar, corrigir, ou substituir, às suas expensas, no todo ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução e/ou de materiais empregados;

c) assumir inteira responsabilidade civil, administrativa e penal por qualquer dano ou prejuízo causado ao **BDMG** ou a terceiros, independentemente de sua culpa ou dolo, não reduzindo ou excluindo esta responsabilidade a fiscalização feita pelo **BDMG**;

d) não utilizar qualquer nome, marca, logotipo, símbolo ou imagem de propriedade do **BDMG**, nem mesmo fazer qualquer menção ao nome ou imagem do **BDMG**, inclusive para fins de publicidade própria, sem prévia e expressa autorização do **BDMG**;

e) manter, durante toda a vigência do contrato, todas as condições e documentações exigidas para a contratação;

f) aceitar, por parte do **BDMG**, em todos os aspectos, a fiscalização da execução do contrato;

g) prestar os esclarecimentos que forem solicitados pelo **BDMG**, bem como dar ciência a este, imediatamente e por escrito, de qualquer anormalidade que verificar;

h) comunicar imediatamente ao **BDMG** qualquer alteração ocorrida na conta bancária, endereço físico e eletrônico bem como quaisquer outras informações necessárias para recebimento de correspondências, físicas ou eletrônicas, ou efetividade do pagamento e da comunicação com o **BDMG**;

i) seguir as disposições do Código de Ética do BDMG, que se encontra disponível no site deste banco de desenvolvimento;

j) promover mecanismos para proteção de dados pessoais em conformidade com a Lei Federal nº 13.709/18 – LGPD;

j.1) As definições relacionadas aos dados pessoais são interpretadas de acordo com a LGPD, visando assegurar a proteção dos dados pessoais e o sigilo das informações protegidas.

k) pelo que determina a Resolução BACEN nº 4.557/17, art. 33, § 1º:

I – atender ao disposto nos incisos IV, VII, VIII, IX e X da resolução,

INFORMAÇÃO CONTROLADA

II – conceder ao **BDMG** acesso aos dados e informações sobre os serviços prestados,

III – conceder ao Banco Central do Brasil permissão de acesso a termos firmados, documentação e informações referentes aos serviços prestados e dependências da CONTRATADA.

l) recrutar, em seu nome e sob sua inteira e exclusiva responsabilidade, os profissionais necessários à execução dos serviços, observada a idoneidade moral e profissional, respondendo exclusivamente pelos

encargos sociais, trabalhistas, previdenciários e fiscais previstos na legislação vigente e por quaisquer outros que decorram de sua condição de empregadora ou contratante, inexistindo qualquer vínculo empregatício, de subordinação ou de solidariedade entre o BDMG e os profissionais por ela alocados na execução do objeto;

m) responsabilizar-se integralmente pelo pagamento de multas relativas a encargos sociais, trabalhistas, previdenciários, fiscais e comerciais resultantes da má gestão dos serviços contratados, da sua imperfeita execução ou do descumprimento, parcial ou integral, de quaisquer dos deveres contratuais assumidos;

n) ressarcir o BDMG por eventuais danos, extravios de documentos e prejuízos que lhe forem causados por seus empregados ou prepostos na execução deste contrato, bem como pelos tributos, impostos e taxas que o Banco venha a recolher junto à fazenda pública na condição de responsável tributário, nos termos do art. 128 do Código Tributário Nacional;

o) refazer ou corrigir, imediatamente após o comunicado, com absoluta prioridade e às suas expensas, os serviços justificadamente recusados pelo BDMG;

p) comunicar ao BDMG, por escrito e no prazo máximo de 10 (dez) dias úteis, quaisquer alterações em seu contrato ou estatuto social, anexando os documentos comprobatórios das modificações ou da consolidação;

q) abster-se de apresentar ou de cobrar, sob qualquer alegação, inclusive de fato superveniente, despesa diversa da expressamente prevista neste contrato;

r) manter, durante toda a vigência, canais ativos de telefonia fixa e móvel, correio eletrônico, videoconferência e demais recursos tecnológicos necessários à prestação dos serviços, em regime 24x7x365, na forma dos itens 8.6 e 8.7 do Anexo IV-A – Termo de Referência – Requisitos;

s) cumprir em sua integralidade os demais requisitos e obrigações previstos no Anexo IV-A – Termo de Referência – Requisitos.

CLÁUSULA 9 - DA SEGURANÇA CIBERNÉTICA

9.1. A **CONTRATADA** deve manter sempre o cumprimento dos requisitos legais, regulamentares ou contratuais relacionados com a segurança da informação, com especial enfoque no que se refere à

INFORMAÇÃO CONTROLADA

proteção de dados, incluindo os de natureza pessoal, em todos os locais onde a sua informação é armazenada e tratada.

9.1.1. A **CONTRATADA** deve identificar os possíveis riscos e impactos que possam existir no serviço, auxiliando na validação das medidas compensatórias adotadas para eliminar ou mitigar o risco.

9.1.2. A **CONTRATADA** armazenará apenas as informações permitidas e se absterá de armazenar qualquer informação sem o conhecimento e autorização expressa do **BDMG**.

9.1.3. A **CONTRATADA** deve tratar os dados e informações do **BDMG** com absoluta confidencialidade e cumprir sempre as instruções recebidas em relação à sua finalidade, conteúdo, uso e processamento.

9.1.4. A **CONTRATADA** deve remover e destruir de forma adequada e segura todas as instâncias de quaisquer informações ou dados sigilosos do **BDMG** para garantir que as transações e outros dados não possam ser recuperados por pessoas não autorizadas.

9.1.5. A **CONTRATADA** poderá ser sujeita a auditorias nas quais se verifique o correto cumprimento das práticas de segurança da informação e deverá fornecer as provas e informações necessárias para essa verificação.

9.1.5.1. Em caso de constatação de alguma falha ou descumprimento, a **CONTRATADA** deverá aplicar as medidas corretivas necessárias para eliminar ou mitigar o risco detectado.

9.2. A **CONTRATADA** deve monitorar as permissões de acesso às informações do **BDMG**, garantindo que somente sejam acessíveis às pessoas autorizadas para o desempenho do serviço contratado.

9.2.1. A **CONTRATADA** deve ter um procedimento de revisão periódica sobre as permissões e controles de acesso configurados nos sistemas que atendem ao **BDMG**.

9.2.2. A **CONTRATADA** assegurará, no âmbito do seu processo interno de gestão de acessos, que qualquer acesso às informações do **BDMG** é revogado quando não for mais necessário para a prestação do serviço.

9.3. A **CONTRATADA** deve notificar imediatamente o **BDMG** sobre incidentes de segurança cibernética que afetem seus dados e/ou serviços, assim que forem detectados.

9.3.1. Em caso de incidente de segurança da informação relacionado ao serviço prestado pela **CONTRATADA**, este deve prestar todo apoio necessário, o que não exclui eventual responsabilidade por perdas e danos.

9.4. Tratamento de dados pessoais. Para os fins da Lei nº 13.709/2018 (LGPD), o BDMG figura como CONTROLADOR e a CONTRATADA como OPERADORA dos dados pessoais a que tiver acesso em razão deste contrato, obrigando-se a:

a) realizar o tratamento exclusivamente para a finalidade de execução do objeto e nos estritos limites das instruções documentadas do BDMG, vedado o tratamento para finalidade própria, comercial, estatística, de desenvolvimento de produtos ou de treinamento de modelos, ainda que

sob a forma de dados agregados, anonimizados ou de inteligência de ameaças, salvo autorização prévia, expressa e específica do Banco;

b) adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, observados os princípios da segurança e da prevenção do art. 6º, incisos VII e VIII, da LGPD;

c) restringir o acesso aos dados pessoais aos profissionais estritamente necessários à execução dos serviços, previamente identificados ao BDMG e signatários do termo individual de sigilo exigido no subitem 10.8;

d) não compartilhar, transferir, ceder ou franquear acesso a dados pessoais do BDMG a terceiros, salvo mediante autorização prévia, expressa e específica do Banco, respondendo integralmente pelos atos de eventuais suboperadores autorizados;

e) comunicar ao BDMG, por escrito e imediatamente, qualquer incidente de segurança que envolva dados pessoais, em prazo que assegure ao Banco o cumprimento do prazo de 3 (três) dias úteis fixado pela Resolução CD/ANPD nº 15/2024 para comunicação à Autoridade Nacional de Proteção de Dados e aos titulares, fornecendo, desde logo, a descrição dos dados atingidos, dos titulares envolvidos, das medidas adotadas e dos riscos decorrentes;

f) auxiliar o BDMG no atendimento a requisições de titulares, a determinações da Autoridade Nacional de Proteção de Dados e a demandas de órgãos de controle e de regulação, nos prazos por ele indicados;

g) eliminar os dados pessoais ao término do tratamento ou da vigência contratual, na forma do subitem 3.9 deste contrato e dos itens 14.4 e 14.5 do Anexo IV-A – Termo de Referência – Requisitos, ressalvadas as hipóteses de guarda obrigatória previstas no art. 16 da LGPD, comprovando formalmente a eliminação ao BDMG;

h) manter registro das operações de tratamento realizadas por conta do BDMG e disponibilizá-lo ao Banco sempre que solicitado.

9.4.1. A CONTRATADA responde pelos danos decorrentes do descumprimento das obrigações da legislação de proteção de dados ou das instruções documentadas do BDMG, nos termos dos arts. 42 a 45 da LGPD, sem prejuízo das glosas, das sanções contratuais e da execução da garantia de execução contratual.

9.5. Localização, processamento e armazenamento dos dados. Os dados do BDMG tratados em ambiente da CONTRATADA, do fabricante das soluções por ela fornecidas ou de provedores de nuvem por qualquer deles contratados — incluídos o inventário de ativos, os resultados de varreduras, os registros da ferramenta de ITSM, as evidências e os artefatos das campanhas de Caça a Ameaças e as respectivas cópias de segurança — serão armazenados e processados no Brasil ou em país que disponha de convênio para troca de informações entre o Banco Central do Brasil e a respectiva autoridade supervisora, na forma dos arts. 15 e 16 da Resolução CMN nº 4.893/2021, conforme relação disponível em https://www.bcb.gov.br/estabilidadefinanceira/memorandosupervisao.

INFORMAÇÃO CONTROLADA

9.5.1. A CONTRATADA informará ao BDMG, na ocasião do Plano de Implantação e sempre que houver alteração, os países e as regiões em que os dados do Banco poderão ser armazenados, processados e gerenciados, bem como a identificação dos provedores de nuvem envolvidos, ficando qualquer alteração sujeita à anuência prévia do BDMG.

9.5.2. É vedado à CONTRATADA replicar, copiar ou realizar cópias de segurança dos dados do BDMG fora do território brasileiro sem autorização prévia, expressa e específica do Banco, observado, em qualquer hipótese, o disposto no subitem 9.5.

9.5.3. Eventual transferência internacional de dados pessoais observará as hipóteses e as salvaguardas dos arts. 33 a 36 da Lei nº 13.709/2018, cabendo à CONTRATADA formalizar as garantias exigidas e comprová-las ao BDMG.

9.5.4. Serão observados, ainda, a partir do ponto de entrada e de saída dos dados do BDMG no ambiente da CONTRATADA ou do fabricante:

a) a inviolabilidade e o sigilo do fluxo das comunicações do BDMG e das suas comunicações privadas armazenadas, salvo por ordem judicial, na forma da lei;

b) o não fornecimento a terceiros de dados do BDMG, inclusive registros de conexão e de acesso a aplicações, salvo nas hipóteses previstas em lei ou mediante autorização expressa do Banco;

c) a vedação de acesso aos dados do BDMG, pela CONTRATADA ou por terceiros, sem prévia autorização, salvo por ordem judicial, na forma da lei.

9.5.5. A CONTRATADA franqueará ao BDMG o acesso a certificações e a relatórios de auditoria independente relativos aos procedimentos e controles empregados na prestação dos serviços, inclusive os do provedor de nuvem utilizado.

CLÁUSULA 10 - CONFIDENCIALIDADE

10.1. A **CONTRATADA** manterá o mais absoluto sigilo sobre as operações, dados, materiais, pormenores, informações, documentos, especificações técnicas ou comerciais, inovações e aperfeiçoamentos tecnológicos ou comerciais, contidos em quaisquer documentos e/ou mídias, inclusive programas, rotinas ou arquivos, do **BDMG**, de seus clientes, empregados ou de terceiros, especialmente as informações cobertas pelo sigilo bancário, que lhe sejam, voluntária ou involuntariamente, reveladas, fornecidas, comunicadas, adquiridas (seja verbalmente ou por escrito, em forma eletrônica, textos desenhos, fotografias, gráficos, projetos, plantas ou qualquer outra forma), independentemente da classificação de sigilo conferida pelo **BDMG** a tais documentos, devendo abster-se de copiar, reproduzir, vender, ceder, licenciar, comercializar, transferir ou de outra forma alienar, divulgar, revelar, reproduzir, disponibilizar tais informações a terceiros ou utilizá-las para quaisquer fins não atinentes ao objeto do contrato.

10.2. A **CONTRATADA** deverá, na hipótese de término ou rescisão deste contrato ou ainda mediante solicitação do **BDMG**, observado, nesse último caso, o prazo de até 05 (cinco) dias úteis contados do seu recebimento, devolver todo o material (ainda que em mídias), bem como suas respectivas cópias, que, sob qualquer forma, estejam em seu poder ou de qualquer integrante da equipe de trabalho.

INFORMAÇÃO CONTROLADA

Deverá, ainda, nas mesmas hipóteses, apagar e ou destruir as informações de quaisquer bancos de dados, sejam físicos ou virtuais.

10.3. Ficam ressalvadas, desde que mantida a confidencialidade, a devolução de cópias das informações e documentos que:

a) em obediência à legislação vigente ou às normas regulamentares aplicáveis devam ser mantidos pela **CONTRATADA**;

b) tenham sido utilizados para comprovação de que os serviços prestados pela **CONTRATADA** ao **BDMG** atendem aos requisitos do contrato e às normas e leis aplicáveis.

10.4. Todas as informações recebidas pela **CONTRATADA** para execução da prestação do objeto contratual, inclusive aquelas cobertas por confidencialidade nos termos desta cláusula, poderão ser disponibilizadas aos representantes legais e profissionais integrantes de sua equipe de trabalho alocada aos serviços do **BDMG**, direta ou indiretamente, cabendo também a estes os mesmos compromissos de sigilo assumidos pela **CONTRATADA**.

10.5. A **CONTRATADA** responsabilizar-se-á, para todos os fins e efeitos, por tais representantes legais e profissionais quanto às obrigações de sigilo assumidas.

10.6. A **CONTRATADA** deverá indenizar, defender e assegurar ao **BDMG**, quaisquer perdas, danos, custos, despesas, responsabilidades, ações, reclamações e procedimentos decorrentes, direta ou indiretamente, do descumprimento das obrigações de sigilo, inclusive sigilo bancário, sem prejuízo das medidas liminares ou cautelares cabíveis em relação ao seu descumprimento efetivo ou potencial.

10.7. As obrigações de sigilo subsistirão ao término do contrato ou em caso de rescisão.

O dever de sigilo estabelecido nos subitens acima não será aplicável a quaisquer informações que pertençam ao domínio público anteriormente ao seu recebimento pela **CONTRATADA**; ou posteriormente ao seu recebimento pela **CONTRATADA**, desde que não tenham recebido tal qualidade em decorrência de violação das obrigações de sigilo; ou, ainda, caso sejam reveladas pela **CONTRATADA**, por força de lei ou por ordem de autoridade competente.

10.8. Além da responsabilidade civil da **CONTRATADA**, todos os profissionais por ela alocados na execução dos serviços, inclusive o Analista de Segurança Sênior de Nível 3 (N3), deverão assinar o Termo de Compromisso e Manutenção de Sigilo (NDA) em caráter individual e pessoal.

10.8.1. O acesso aos ambientes do **BDMG** só será concedido após a entrega de cópia assinada dos referidos termos ao Fiscal do Contrato.

10.8.2. O dever de sigilo subsiste mesmo após o desligamento do profissional da **CONTRATADA** ou após o encerramento do contrato com o **BDMG**.

CLÁUSULA 11 - POLÍTICA ANTICORRUPÇÃO

11.1. A **CONTRATADA** declara e garante que:

a) se obriga, sob as penas previstas no contrato e na legislação aplicável, a observar e cumprir rigorosamente todas as leis cabíveis, especialmente à legislação brasileira anticorrupção;

b) não está envolvida ou irá se envolver, direta ou indiretamente, por meio de seus representantes, administradores, diretores, conselheiros, sócios ou acionistas, assessores, consultores, partes relacionadas, durante o cumprimento das obrigações previstas no contrato, em qualquer atividade ou prática que constitua uma infração ao termo da lei anticorrupção.

c) notificará prontamente ao **BDMG** sobre qualquer investigação ou procedimento instaurados por autoridade governamental envolvendo seus representantes, administradores, diretores, conselheiros, sócios ou acionistas, assessores, consultores, direta ou indiretamente em virtude de denúncias de suborno e/ou corrupção, relacionados ao contrato advindo da licitação.

d) direta ou indiretamente, não ofereceu, prometeu, pagou ou autorizou o pagamento em dinheiro, deu ou concordou em dar presentes ou qualquer objeto de valor e, durante a vigência do contrato, não irá ofertar, prometer, pagar ou autorizar o pagamento em dinheiro, dar ou concordar em dar presentes ou qualquer objeto de valor a qualquer pessoa ou entidade, pública ou privada, com o objetivo de beneficiar ilicitamente ao **BDMG** e/ou seus negócios.

e) direta ou indiretamente, não irá receber, transferir, manter, usar ou esconder recursos que decorram de qualquer atividade ilícita, bem como não irá contratar como empregado ou de alguma forma manter relacionamento profissional com pessoas físicas ou jurídicas envolvidas em atividades criminosas, em especial pessoas investigadas pelos delitos previstos nas leis anticorrupção e de lavagem de dinheiro.

f) se obriga a notificar prontamente, por escrito, ao **BDMG** a respeito de qualquer suspeita ou violação do disposto nas leis anticorrupção, e ainda de participação em práticas de suborno ou corrupção, assim como o descumprimento de qualquer declaração prevista nesta cláusula.

11.2. O não cumprimento pela **CONTRATADA** das leis anticorrupção, bem como do conteúdo desta cláusula, será considerado uma infração grave e conferirá ao **BDMG** o direito de, agindo de boa-fé, declarar rescindido imediatamente o contrato sem qualquer ônus ou penalidade, sendo a **CONTRATADA** responsável por eventuais perdas e danos.

CLÁUSULA 12 - DA PREVENÇÃO AOS CRIMES DE LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO

12.1. A **CONTRATADA** declara ter pleno conhecimento da Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo do Contratante, fundamentada na Circular do Banco Central do Brasil de n. 3.978, de 23 de janeiro de 2020, a qual dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, da Lei nº 9.613, de 03 de março de 1998, e da Lei nº 13.260, de 16 de março de 2016, comprometendo-se a observar os comandos desses normativos, bem como de toda a legislação pertinente ao tema.

12.2. A **CONTRATADA** declara que não praticou nenhum dos ilícitos previstos na legislação que regulamenta a prevenção à lavagem de dinheiro e financiamento ao terrorismo, ou estão sob investigação em relação a eventual cometimento de infrações previstas na menciona legislação.

INFORMAÇÃO CONTROLADA

12.3. As declarações realizadas pela **CONTRATADA** nesta cláusula também abrangem seus administradores, empregados, prepostos e terceiros a ela relacionados, responsabilizando-se todos pela fiel observância dos dispositivos legais em questão.

12.4. A **CONTRATADA** se obriga a notificar prontamente, por escrito, ao **BDMG** a respeito de qualquer suspeita ou violação do disposto nas normas pertinentes às Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo, assim como o descumprimento de qualquer declaração prevista nesta cláusula.

12.5. O não cumprimento pela **CONTRATADA** das normas pertinentes às Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo será considerado uma infração grave ao contrato e conferirá ao **BDMG** o direito de, agindo de boa-fé, declarar rescindido imediatamente o contrato, sem qualquer ônus ou penalidade, sendo a **CONTRATADA** responsável por eventuais perdas e danos.

12.6. A CONTRATADA deverá apresentar, no ato da assinatura e anualmente, declaração formal indicando a existência ou não de sócios, administradores ou prepostos que se enquadrem como Pessoas Politicamente Expostas (PEP), conforme a Circular do Banco Central do Brasil de n. 3.978, de 23 de janeiro de 2020.

12.7. A omissão ou falsidade nesta declaração constitui falta grave, passível de rescisão imediata e aplicação de penalidades.

CLÁUSULA 13 - FISCALIZAÇÃO E ACOMPANHAMENTO DO CONTRATO

13.1. Caberá ao Superintendente da Superintendência de Tecnologia da Informação executar a gestão do contrato e ao empregado, especificamente designado, exercer a função de fiscal do contrato, visando à observância do fiel cumprimento das exigências contratuais.

13.2. O Fiscal do Contrato, além de outras obrigações constantes das normas pertinentes e deste contrato, deverá manter anotações e registros de todas as ocorrências e determinar o que for necessário à regularização das falhas ou problemas observados, bem como provocar alterações contratuais, caso sejam necessárias e atestar a plena execução do contrato.

13.3. A gestão, acompanhamento e fiscalização de que trata esta cláusula não excluem nem reduzem a responsabilidade da CONTRATADA pelo correto cumprimento das obrigações decorrentes da contratação.

13.4. A CONTRATADA entregará, em até 05 (cinco) dias úteis após a data de assinatura deste instrumento contratual, carta de preposição, devidamente assinada também pelo preposto qualificado e nomeado, declarando expressamente que a pessoa indicada estará designada para, em seu nome:

a) participar de reuniões e assinar as respectivas atas, vinculando a **CONTRATADA** às decisões e determinações nelas consignadas;

b) receber, mediante correspondência eletrônica, correios ou qualquer outro meio de comunicação, solicitações, instruções e notificações, estas:

i. de descumprimento de cláusula contratual;

ii. de aplicação de penalidade;

INFORMAÇÃO CONTROLADA

iii. de rescisão;
iv. de convocação;
v. referentes a tomada de providências para ajustes e aditivos contratuais; e
vi. quaisquer outras que lhe imponham ou não prazo de resposta, inclusive os relacionados a processo administrativo instaurado pelo **BDMG**.

c) representá-la em todos os demais atos que se relacionem à finalidade específica da nomeação, qual seja a ampla gestão da contratação, no que couber à CONTRATADA.

13.5. Até a data de assinatura deste instrumento contratual, o BDMG enviará à CONTRATADA, por e-mail, modelo de carta de preposição a qual abrangerá exclusivamente o expresso nesta cláusula.

13.6. A não apresentação da carta de constituição de preposto, devidamente preenchida e assinada, no prazo determinado para tanto, será considerado descumprimento de obrigação contratual, sujeitando a CONTRATADA às penalidades cabíveis.

13.7. Na qualificação do preposto, a CONTRATADA deverá informar número de telefone e e-mail, aptos para contato direto com aquele, além de documento de identificação civil válido e número de inscrição no Cadastro de Pessoas Físicas.

13.8. O preposto ficará responsável pela gestão dos aspectos administrativos, legais e técnicos do contrato pertinentes à CONTRATADA, e acompanhar de forma contínua e periódica a execução, relacionando-se diretamente com o Fiscal do Contrato.

CLÁUSULA 14 - VEDAÇÕES

14.1. É vedado à CONTRATADA:

a) caucionar ou utilizar o contrato para qualquer operação financeira;

b) transferir ou ceder a terceiros o objeto contratado, ainda que parcialmente.

14.2. Poderão excluir-se da hipótese da alínea b do subitem acima, a critério exclusivo do BDMG, os casos de fusão, cisão e incorporação da CONTRATADA, ainda que parciais, bem como as subcontratações expressamente permitidas neste contrato.

CLÁUSULA 15 - INADIMPLEMENTO

15.1. São considerados inadimplentes:

a) a CONTRATADA, caso deixe de cumprir qualquer das cláusulas e condições estipuladas no contrato ou interrompa sua execução sem motivo justificado;

b) o BDMG se, por motivos alheios à CONTRATADA, der causa à paralisação total do objeto contratado, obrigando-se ao pagamento proporcional dos trabalhos até então realizados, ressalvados os casos fortuitos ou de força maior.

15.2. A tolerância das partes relativamente a qualquer atraso ou inadimplência não importará em alteração contratual ou novação, cabendo-lhes exercer seus direitos a qualquer tempo.

CLÁUSULA 16 - SANÇÕES CONTRATUAIS

INFORMAÇÃO CONTROLADA

16.1. A inexecução parcial ou total das condições contratuais pela **CONTRATADA** permitirá a aplicação das seguintes sanções pelo **BDMG**:

a) advertência;

b) multa;

c) suspensão temporária do direito de licitar e contratar com o **BDMG** pelo prazo de até 2 (dois) anos.

16.2. Para aplicação das sanções previstas nas alíneas b) e c) do subitem acima, o **BDMG** instaurará processo administrativo para apuração dos fatos, no qual serão garantidos os princípios da ampla defesa e contraditório.

16.3. A **CONTRATADA** poderá apresentar defesa no prazo de até 10 (dez) dias úteis a partir da ciência da instauração do processo que será direcionada para o contato eletrônico do preposto e, se houver, para outros contatos de uso rotineiro para as comunicações com o **BDMG**, ou, na impossibilidade técnica deste encaminhamento, por meio de publicação na Imprensa Oficial de Minas Gerais.

16.4. Poderá ser aplicada advertência nos casos em que os atos da **CONTRATADA** não causarem nenhum prejuízo ao **BDMG**, suas instalações, pessoas, imagem, meio ambiente ou a terceiros, limitando-se apenas aos casos de conduta que impeçam a plena execução do contrato.

16.4.1. Será igualmente aplicada a sanção de advertência nas hipóteses de:

a) não atingimento de um mesmo nível mínimo de serviço durante 3 (três) meses consecutivos ou 5 (cinco) meses alternados, apurados em período de 12 (doze) meses;

b) reincidência de atraso superior a 15 (quinze) dias em relação ao prazo fixado para o início da execução ou para a entrega dos produtos e relatórios previstos neste contrato e no Anexo IV-A – Termo de Referência – Requisitos, no período de 6 (seis) meses contados da primeira ocorrência;

c) inobservância de outras normas contidas no edital ou no instrumento contratual de que não advenham prejuízos comprovados ao BDMG.

16.4.2. A aplicação de 3 (três) advertências no período de 12 (doze) meses sujeitará a CONTRATADA à multa de 10% (dez por cento) calculada sobre o valor mensal do serviço, sem prejuízo das glosas previstas no item 12.25 do Anexo IV-A – Termo de Referência – Requisitos, com as quais não se confunde, nos termos da nota IV do mesmo item.

16.5. A reincidência da sanção de advertência poderá ensejar a aplicação da penalidade de suspensão.

16.6. Para aplicação da sanção de advertência não é devida a abertura de procedimento administrativo, sendo obrigatória a motivação do ato sancionador pelo gestor ou fiscal do contrato.

16.7. Ficam estabelecidos os seguintes valores de multas, aplicáveis, a critério do **BDMG**, e após regular processo administrativo:

a) Multa moratória à razão de 0,3% (três décimos por cento) por dia de atraso na entrega do objeto da contratação, calculada sobre o valor da parcela mensal dos itens 1 e 2 do quadro de itens do subitem

INFORMAÇÃO CONTROLADA

1.1 do Anexo IV-A – Termo de Referência – Requisitos, limitada a 30 (trinta) dias, após os quais o contrato poderá ser rescindido e poderá ser aplicada a multa compensatória.

b) Multa, por ocorrência, de 10% (dez por cento) sobre o valor da fatura, em caso de descumprimento de qualquer outra condição deste contrato.

16.8. Multa compensatória de 10% (dez por cento), calculada sobre o valor total do contrato, na hipótese de rescisão contratual por culpa ou desistência da **CONTRATADA**, sem prejuízo da execução da garantia de execução contratual e da reparação dos danos apurados.

16.9. O valor das multas aplicadas à **CONTRATADA**, após regular processo administrativo, será descontado do pagamento, devendo a **CONTRATADA** recolher a diferença no prazo máximo de 03 (três) dias úteis, a contar da aplicação da sanção, se necessário.

16.10. Fica desde já ajustado que todo e qualquer valor que vier a ser imputado pelo **BDMG** à **CONTRATADA**, a título de multa, reveste-se das características de liquidez e certeza para efeitos de execução judicial, nos termos do art. 783 do Código de Processo Civil.

16.11. Reveste-se das mesmas características qualquer obrigação definida nesse instrumento como de responsabilidade da **CONTRATADA** e que, por eventual determinação judicial ou administrativa, venha a ser paga pelo **BDMG**.

16.12. O pagamento das multas previstas neste contrato não exime a **CONTRATADA** da responsabilidade pela reparação de eventuais danos, perdas ou prejuízos causados ao **BDMG**.

16.13. As sanções de multa e demais sanções poderão ser aplicadas cumulativamente.

16.14. O **BDMG** poderá, após regular processo administrativo, aplicar a sanção de suspensão temporária de participação em licitação e contratação, caso a **CONTRATADA**:

a) sofra condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos: suspensão por 24 meses;

b) pratique atos ilícitos visando a frustrar os objetivos da contratação: suspensão por 24 meses;

c) demonstre não possuir idoneidade para contratar com o **BDMG** em virtude de atos ilícitos praticados: suspensão por 24 meses;

d) apresente documentação falsa exigida para a contratação: suspensão por 24 meses;

e) enseje o retardamento da execução do objeto contratado: suspensão de 03 a 24 meses, a ser definido em face da gravidade do fato e mediante motivação da autoridade superior;

f) falhe na execução do objeto contratado: suspensão de 03 a 24 meses, a ser definido em face da gravidade do fato e mediante motivação da autoridade superior;

g) cometa fraude na execução do objeto contratado: suspensão por 24 meses;

h) comporte-se de modo inidôneo, inclusive com a prática de atos lesivos à Administração Pública previstos na Lei Federal nº 12.846/2013: suspensão por 24 meses;

i) se torne reincidente nas penalidades de advertência e multa: suspensão de 03 a 24 meses, a ser definido em face da gravidade do fato e mediante motivação da autoridade superior.

INFORMAÇÃO CONTROLADA

16.14.1. A aplicação da sanção de suspensão temporária de participação em licitação e contratação à **CONTRATADA** ensejará a rescisão unilateral do contrato.

CLÁUSULA 17 - RESCISÃO

17.1. O contrato poderá ser rescindido unilateralmente pelo BDMG, assegurada a defesa prévia, quando ocorrer:

a) o não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;
b) a decretação de falência ou a instauração de insolvência civil;
c) o descumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, que proíbe o trabalho noturno, perigoso ou insalubre a menores de 18 anos e qualquer trabalho a menores de 16 anos, salvo na condição de aprendiz, a partir de 14 anos;
d) a prática de atos lesivos à Administração Pública previstos na Lei Federal nº 12.846/2013;
e) a inobservância da vedação ao nepotismo;
f) a prática de atos que prejudiquem ou comprometam à imagem ou reputação do BDMG, direta ou indiretamente.

17.2. O contrato poderá ser rescindido por acordo entre as partes, mediante comunicação escrita encaminhada com antecedência mínima de 90 (noventa) dias e concordância escrita e fundamentada do BDMG, assegurada, em qualquer hipótese, a execução integral da transição assistida prevista no subitem 3.8 deste contrato e no item 14.3 do Anexo IV-A – Termo de Referência – Requisitos.

17.2.1. A CONTRATADA não interromperá a prestação dos serviços antes de concluída a transição assistida e formalizado o handover técnico, ainda que já encerrado o prazo de vigência, sob pena de caracterização de inexecução contratual, com aplicação das sanções da CLÁUSULA 16 e execução da garantia de execução contratual, sem prejuízo da reparação dos danos.

17.3. O contrato poderá ser rescindido por determinação judicial.

17.4. A rescisão unilateral será devidamente fundamentada nos autos do processo administrativo que a precederá, no qual serão garantidos os princípios da ampla defesa e contraditório.

17.5. Os efeitos da rescisão do contrato serão operados a partir da comunicação oficial à CONTRATADA, mediante encaminhamento ao contato eletrônico do preposto e/ou, se for o caso, para outro contato eletrônico de uso rotineiro para as comunicações com o BDMG ou, na impossibilidade deste encaminhamento, por meio de publicação na Imprensa Oficial de Minas Gerais.

17.6. Em caso de rescisão sem culpa da CONTRATADA, a ela serão devidos os valores correspondentes ao objeto efetivamente realizado, mediante comprovação da efetiva execução, observados eventuais descontos em razão de penalização ou outro ajuste decorrente do contrato.

CLÁUSULA 18 - DECLARAÇÕES

18.1. A CONTRATADA declara expressamente, para todos os fins e efeitos, que:

a) inexistem fatos impeditivos à sua contratação pelo BDMG, prescritos na legislação específica, inclusive os previstos no artigo 11 do Regulamento de Licitações e Contratos do BDMG;

INFORMAÇÃO CONTROLADA

b) em nenhuma das suas dependências ou estabelecimentos ocorre trabalho noturno, perigoso ou insalubre por menores de 18 (dezoito) anos ou qualquer trabalho por menores de 16 (dezesseis) anos, salvo na condição de aprendiz, na forma da Lei;

c) informará imediatamente ao BDMG a ocorrência de qualquer das situações previstas nos subitens acima;

d) autoriza, para fins das obrigações e condições desta contratação, a coleta e o tratamento, pelo BDMG, dos dados pessoais constantes de quaisquer dos seus documentos entregues para a contratação ou durante a vigência do contrato, observada a Política de Privacidade e Proteção de Dados Pessoais do BDMG e da legislação aplicável.

CLÁUSULA 19 - GARANTIA DE EXECUÇÃO CONTRATUAL

19.1. A CONTRATADA apresentará ao BDMG, no prazo máximo de 10 (dez) dias úteis contados da data de assinatura do instrumento contratual, comprovante de prestação de garantia correspondente a 5% (cinco por cento) do valor total do contrato, podendo optar por caução em dinheiro, seguro-garantia ou fiança bancária.

19.2. A garantia terá validade durante toda a execução do contrato e por mais 3 (três) meses após o término da vigência contratual, e será renovada a cada prorrogação efetivada.

19.3. A garantia, na modalidade escolhida pela CONTRATADA, assegurará o pagamento de:

a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

b) multas aplicadas pelo BDMG à CONTRATADA;

c) prejuízos diretos causados ao BDMG e a terceiros, decorrentes de culpa ou dolo durante a execução do contrato; e

d) obrigações previdenciárias e trabalhistas não honradas pela CONTRATADA.

19.4. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no subitem 19.3.

19.5. A CONTRATADA obriga-se a:

a) readequar ou renovar, nas mesmas condições originais e no prazo de até 10 (dez) dias úteis contados da notificação, prorrogáveis por igual período a critério do BDMG, a garantia prestada, no caso de alteração do valor total do contrato ou de prorrogação de sua vigência; e

b) repor o valor da garantia que venha a ser utilizado pelo BDMG, de forma que volte a representar 5% (cinco por cento) do valor total atualizado do contrato.

19.6. A garantia em dinheiro será efetuada em conta específica em favor do BDMG, com correção monetária pelo Índice Nacional de Preços ao Consumidor Amplo – IPCA, divulgado pelo IBGE, acumulado no período.

INFORMAÇÃO CONTROLADA

19.7. O número do contrato garantido e/ou assegurado deverá constar dos instrumentos de garantia ou de seguro apresentados pelo garantidor e/ou segurador.

19.8. O BDMG não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses, devidamente comprovadas:

a) caso fortuito ou força maior;

b) alteração, sem prévio conhecimento da seguradora ou do fiador, das obrigações contratuais;

c) descumprimento das obrigações pela CONTRATADA decorrente de atos ou fatos praticados pelo BDMG;

d) atos ilícitos dolosos praticados por empregados do BDMG no âmbito da execução do contrato.

19.8.1. Caberá ao BDMG apurar a isenção de responsabilidade prevista no subitem 19.8, não sendo a entidade garantidora parte no processo administrativo instaurado pelo BDMG.

19.8.2. Não serão aceitas garantias que incluam isenções de responsabilidade diversas das previstas no subitem 19.8, nem que vinculem a sua execução ou o seu resgate à rescisão deste contrato.

19.9. Para efeito de execução da garantia, os inadimplementos contratuais serão comunicados pelo BDMG à CONTRATADA e/ou à instituição garantidora no prazo de até 90 (noventa) dias após o término do processo administrativo relacionado à aplicação da sanção específica.

19.10. Será considerada extinta a garantia, de modo alternativo:

a) com a devolução da apólice, da carta de fiança ou da autorização para o levantamento das importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do BDMG, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato; ou

b) 90 (noventa) dias após a extinção do contrato.

19.11. O descumprimento do prazo previsto no subitem 19.1 sujeitará a CONTRATADA a multa moratória diária de 0,05% (cinco centésimos por cento), calculada sobre o valor total do contrato, até o limite de 0,5% (cinco décimos por cento), sem prejuízo das demais sanções previstas na CLÁUSULA 16.

CLÁUSULA 20 - TRATAMENTO DE DADOS PESSOAIS

20.1. Para efeitos do Contrato, o tratamento e proteção de dados pessoais dar-se-ão em conformidade com a Lei Federal nº 13.709/18 – LGPD. As definições relacionadas aos dados pessoais doravante mencionadas deverão ser expressamente referidas e interpretadas de acordo com a citada Lei.

20.2. A contar da assinatura do Contrato e até o seu término, o BDMG indica a CONTRATADA, que aceita, sua indicação, como operador, nos termos do art. 5.º, inciso VII da LGPD, para os fins de tratamento dos dados pessoais estritamente necessários para garantir a execução do Contrato.

20.3. A CONTRATADA executará o contrato em conformidade com as obrigações impostas pela lei mencionada aos operadores de dados pessoais, em especial tomando todas as medidas de segurança relacionadas no art. 6.º, inciso VII e art. 46 da LGPD.

20.4. A CONTRATADA não envolverá qualquer outro operador sem a autorização prévia e escrita do BDMG.

20.5. A CONTRATADA manterá e colocará à disposição do BDMG registro das operações de tratamento de dados pessoais que realizarem em benefício do BDMG, em conformidade com art. 37 da LGPD.

20.6. A CONTRATADA garantirá aos titulares de dados disponibilizados pelo BDMG, quando coletados durante a execução do Contrato, o exercício dos direitos estabelecidos nos artigos 17 a 21 da LGPD, sem prejuízo da garantia de outros direitos estabelecidos em outra legislação aplicável.

20.7. A CONTRATADA notificará o BDMG, em até 24 (vinte e quatro) horas contadas do evento, acerca de qualquer incidente de dados, incluindo vazamento ou comprometimento de dados pessoais relacionadas com o Contrato, inclusive violação acidental ou culposa. A notificação deverá obrigatoriamente conter, no mínimo, a descrição da natureza da violação, o número aproximado de titulares dos dados em questão, o nome e detalhes de contato do encarregado pelo tratamento de dados pessoais, a descrição das prováveis consequências da violação e a descrição das medidas adotadas ou a serem tomadas para mitigar possíveis efeitos adversos.

20.8. A CONTRATADA indenizará ao BDMG quaisquer danos, prejuízos e lucros cessantes, incluindo quaisquer custas judiciais, administrativas e honorários advocatícios, decorrentes do descumprimento das cláusulas de proteção de dados pessoais do Contrato ou do descumprimento legal de obrigações de proteção de dados, ocasionado por ação ou omissão por parte da CONTRATADA, ou por terceiro por ela contratado.

CLÁUSULA 21 - FORO

21.1. As partes contratantes elegem o Foro da Comarca de Belo Horizonte - MG, com renúncia de qualquer outro para dirimir as questões por elas suscitadas.

Por estarem justas e acordadas, e concordando que a assinatura deste instrumento, por meio de processo eletrônico, constituirá assinatura válida, as partes celebram o presente contrato, por seus representantes legais abaixo indicados.

INFORMAÇÃO CONTROLADA

ANEXO IV-A – TERMO DE REFERÊNCIA – REQUISITOS

(Anexo integrante do Anexo IV – Minuta do Instrumento Contratual)

1. REQUISITOS GERAIS DA CONTRATAÇÃO

1.1. O objeto da contratação compreende a prestação de serviços gerenciados de Centro de Operações de Segurança (SOC), em regime de operação contínua 24x7x365 (24 horas por dia, 7 dias por semana, 365 dias por ano), incluindo os seguintes itens:

Item	Descrição	Unidade	Quantidade total
1	Serviço Gerenciado de Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR)	Serviço Mensal	12 (doze)
2	Serviço de Gestão de Vulnerabilidades	Serviço Mensal	12 (doze)
3	Licenças de uso de solução de Gestão de Vulnerabilidades com Gerenciamento de Patches, por 12 (doze) meses	Ativos monitorados	1.200 (mil e duzentos)

1.1.1. Os quantitativos do quadro de itens acima correspondem ao primeiro período contratual, de 14 (quatorze) meses, assim composto: até 2 (dois) meses de implantação, na forma dos subitens 11.1 a 11.11, e 12 (doze) meses de operação continuada.

1.1.2. O objeto compreende dois escopos sucessivos e distintos — implantação e operação — , não havendo item, parcela ou valor destacado a título de implantação, cujos custos deverão estar integralmente diluídos no preço mensal dos itens 1 e 2 do quadro de itens, na forma do subitem 7.1.1 da CLÁUSULA 7 – PAGAMENTO do contrato.

1.1.3. Os itens 1 e 2 do quadro de itens serão remunerados em 12 (doze) parcelas mensais fixas por período contratual de operação, e o item 3 em parcela única, na forma dos subitens 7.1 e 7.1.3 da CLÁUSULA 7 – PAGAMENTO do contrato.

1.1.4. A prorrogação contratual alcança exclusivamente o escopo de operação, em períodos de 12 (doze) meses, ressalvado o último período contratual, de 10 (dez) meses, para que a soma dos períodos — 14, 12, 12, 12 e 10 meses — não exceda 60 (sessenta) meses contados da celebração do contrato. O horizonte máximo da contratação corresponde, portanto, a 58 (cinquenta e oito) parcelas mensais de operação, e não a 60 (sessenta).

1.2. A CONTRATADA prestará serviços gerenciados de Centro de Operações de Segurança da Informação (SOC), por meio de processos, equipes especializadas e soluções tecnológicas adequadas, em regime de operação contínua 24x7x365 (vinte e quatro horas por dia, sete dias por semana e trezentos e sessenta e cinco dias por ano), observadas todas as condições, requisitos, níveis de serviço e demais disposições estabelecidas neste Termo de Referência.

INFORMAÇÃO CONTROLADA

1.3. O SOC da CONTRATADA será responsável pela execução das ações de contenção e resposta aos incidentes de segurança, observados os perfis de acesso e as alçadas de aprovação definidos pelo BDMG, utilizando os recursos e ferramentas de segurança disponibilizados, incluindo, mas não se limitando, ao Microsoft Sentinel, soluções de EDR, firewalls, correio eletrônico, identidade e demais tecnologias integrantes do ambiente monitorado.

1.4. Para os fins deste Termo de Referência:

- Caso de Uso: regra analítica de detecção implementada no Microsoft Sentinel do BDMG;
- Incidente: registro de investigação e tratamento de evento de segurança da informação gerado ou correlacionado no Microsoft Sentinel;
- Chamado: registro correspondente na ferramenta de ITSM utilizada para controle, acompanhamento e medição do atendimento.
- Os termos Caso de Uso, Incidente e Chamado possuem significados distintos e não são intercambiáveis.
- MTTD (Mean Time to Detect): tempo decorrido entre a ocorrência do evento na fonte de dados e a geração do respectivo alerta no Microsoft Sentinel;
- MTTA (Mean Time to Acknowledge): tempo decorrido entre a geração do alerta e o primeiro atendimento efetivo pela equipe da CONTRATADA;
- MTTC (Mean Time to Contain): tempo decorrido entre a geração do alerta e a implementação da contenção efetiva do incidente;
- MTTR (Mean Time to Restore/Recover): tempo decorrido entre a geração do alerta e o restabelecimento do serviço, ativo ou ambiente afetado.
- MTTR-V (Mean Time to Remediate): tempo decorrido entre a confirmação de uma vulnerabilidade e a validação da sua efetiva correção, empregado exclusivamente nos indicadores do Serviço de Gestão de Vulnerabilidades, não se confundindo com o MTTR de incidentes definido acima.

1.5. A prestação dos serviços deverá ocorrer de forma integrada e contínua, assegurando a mensuração dos indicadores de desempenho do SOC, incluindo MTTD, MTTA, MTTC e MTTR, desde a identificação inicial do evento até a completa contenção e recuperação do ambiente.

1.6. O ambiente computacional on-premises e em nuvem do BDMG, descrito no item 6 - ESCOPO E VOLUMETRIA DO AMBIENTE, constitui a base de referência para o dimensionamento dos serviços e elaboração das propostas comerciais pelas licitantes, que deverão considerar todas as características, volumes e requisitos nele informados.

1.7. O **Serviço Gerenciado de Monitoramento, Detecção e Resposta a Incidentes Cibernéticos (MDR)** contemplará o seguinte escopo mínimo:

1.7.1. **Monitoramento de Segurança:**

a) Monitoramento contínuo 24x7x365;

b) Operação por Centro de Operações de Segurança (SOC);

c) Monitoramento de eventos provenientes de:

INFORMAÇÃO CONTROLADA

- Endpoints;
- Servidores físicos e virtuais;
- Serviços em nuvem;
- Dispositivos de rede;
- Soluções de identidade e acesso;
- Firewall, IDS/IPS e demais controles de segurança.

1.7.2. **Detecção de Ameaças:**

a) Detecção de ameaças baseada em comportamento, por meio da identificação de desvios em relação aos padrões normais de operação de usuários, dispositivos, aplicações e serviços;

b) Detecção baseada em Indicadores de Comprometimento (Indicators of Compromise - IoCs), utilizando fontes atualizadas de inteligência de ameaças;

c) Utilização contínua de serviços e fontes de Threat Intelligence para enriquecimento de eventos, correlação de alertas e identificação de ameaças emergentes;

d) Identificação e análise de atividades anômalas que possam indicar tentativas de intrusão, comprometimento de ativos ou uso indevido de recursos tecnológicos;

e) Detecção de ransomware, incluindo comportamentos característicos de criptografia maliciosa, movimentação lateral, exfiltração de dados e demais atividades associadas;

f) Detecção de tentativas de comprometimento de identidades, credenciais privilegiadas e mecanismos de autenticação, abrangendo ambientes locais e em nuvem;

1.7.3. **Caça a Ameaças Cibernéticas (Threat Hunting):**

a) Identificação proativa de ameaças, técnicas de ataque, indicadores de comprometimento, comportamentos maliciosos e riscos ainda não detectados pelos mecanismos convencionais de monitoramento, utilizando como referência, entre outras, as técnicas, táticas e procedimentos (TTPs) descritos no framework MITRE ATT&CK.

1.7.4. **Engenharia de Detecção e Otimização do SIEM:**

a) Concepção, desenvolvimento, implementação, testes, ajuste fino e manutenção contínua de regras analíticas, consultas, casos de uso, playbooks de automação, modelos de correlação e mecanismos de detecção no Microsoft Sentinel do BDMG, com vistas ao aprimoramento contínuo da capacidade de identificação de ameaças, redução de falsos positivos e ampliação da cobertura de detecção alinhada aos cenários de risco e ao framework MITRE ATT&CK.

1.7.5. **Resposta a Incidentes:**

a) Resposta a Incidentes de Segurança Cibernética, em regime 24x7x365, com capacidade de análise, contenção, erradicação e suporte à recuperação de incidentes identificados nos ambientes monitorados;

b) Uma vez identificado um incidente de segurança, a CONTRATADA deverá conduzir as atividades de investigação necessárias para determinar, no mínimo:
   - origem e vetor de ataque;
   - ativos afetados;
   - contas e identidades comprometidas;
   - escopo e impacto do incidente;
   - indicadores de comprometimento (IoCs);
   - técnicas, táticas e procedimentos (TTPs) utilizados pelo agente da ameaça;
   - evidências necessárias para suportar a análise e a tomada de decisão;

c) Executar ações de contenção pré-autorizadas pelo BDMG, que poderão incluir, entre outras:
   - isolamento de estações de trabalho, servidores ou outros ativos;
   - bloqueio de endereços IP, domínios, URLs ou indicadores maliciosos;
   - bloqueio ou encerramento de processos suspeitos;
   - remoção de arquivos maliciosos identificados;
   - desativação ou bloqueio temporário de contas comprometidas;
   - revogação de sessões ativas;
   - bloqueio de credenciais comprometidas;
   - restrição de comunicação entre ativos afetados.

d) Após a contenção, a CONTRATADA deverá apoiar o BDMG nas atividades de erradicação da ameaça, incluindo a identificação da causa raiz, eliminação dos artefatos maliciosos, correção das vulnerabilidades exploradas e implementação das medidas de mitigação necessária;

e) A CONTRATADA deverá apoiar o processo de recuperação dos ativos afetados, acompanhando a normalização dos serviços e verificando a inexistência de indicadores de comprometimento remanescentes;

f) Acionar responsáveis definidos pelo BDMG.

1.7.6. Inteligência de Ameaças (Threat Intelligence): produção, curadoria, enriquecimento e disseminação de inteligência de ameaças cibernéticas relevante ao BDMG e ao setor financeiro, executada por equipe própria e distinta da equipe de Caça a Ameaças (Threat Hunting), na forma do item 3.7.

1.8. O BDMG disponibilizará a plataforma de SIEM/SOAR Microsoft Sentinel necessária à execução dos serviços de MDR, incluindo a assinatura Azure, o licenciamento do Microsoft Sentinel, o workspace Log Analytics e os recursos nativos de automação e orquestração da plataforma, tais como Automation Rules, Playbooks e Azure Logic Apps, arcando com os respectivos custos de ingestão de dados, retenção de logs, processamento e execução desses recursos.

1.8.1. Não integra o objeto desta contratação o fornecimento, pela CONTRATADA, de plataforma de SIEM, SOAR ou de qualquer outra solução que substitua, replique ou duplique funcionalidades nativas do Microsoft Sentinel. A eventual utilização de

ferramentas auxiliares de uso interno da CONTRATADA não poderá constituir requisito indispensável à prestação dos serviços, nem servir como repositório exclusivo de dados, regras de correlação, casos de investigação, indicadores, evidências ou quaisquer informações produzidas no âmbito da execução contratual.

1.8.2. Excetuam-se da vedação prevista a ferramenta de ITSM especificada no item 8 e, quando adotada a alternativa do subitem 9.1, o portal da própria CONTRATADA, cujo fornecimento constitui obrigação da CONTRATADA e integra o objeto desta contratação.

1.9. O Serviço de Gestão de Vulnerabilidades contemplará, no mínimo, o monitoramento contínuo dos ambientes on-premises e em nuvem do BDMG, abrangendo a identificação, classificação, análise e priorização de vulnerabilidades de segurança, bem como a gestão do ciclo de vida de atualizações e correções de software (patches). O serviço incluirá o planejamento, a orquestração, o acompanhamento e a validação da implantação de patches de segurança e demais atualizações nos ativos tecnológicos sob sua cobertura, permanecendo a execução das correções nos ativos do ambiente sob responsabilidade das equipes do BDMG, na forma do subitem 4.3.9. Adicionalmente, o serviço deverá prover mecanismos para acompanhamento da remediação das vulnerabilidades identificadas, geração de relatórios gerenciais e operacionais, e suporte à manutenção da conformidade dos ambientes tecnológicos, com o objetivo de reduzir a superfície de ataque, minimizar a exposição a riscos cibernéticos e fortalecer continuamente a postura de segurança do BDMG.

1.10. A CONTRATADA será responsável pelo licenciamento, implantação, configuração, operação, administração, suporte técnico, atualização de versões e sustentação da solução de Gestão de Vulnerabilidades utilizada na prestação dos serviços.

1.10.1. As licenças de uso da solução de Gestão de Vulnerabilidades permanecerão sob titularidade direta do BDMG durante toda a vigência contratual e, em caso de extinção antecipada do contrato, até o término do período de licenciamento já pago, observado o modelo de licenciamento adotado pelo fabricante.

1.10.2. A solução de Gestão de Vulnerabilidades a ser fornecida deverá atender integralmente aos requisitos funcionais, técnicos, operacionais, de segurança, integração, escalabilidade e suporte estabelecidos neste Termo de Referência, em especial de gerenciamento e instalação de patches.

1.10.3. A CONTRATADA deverá assegurar que a solução seja mantida permanentemente atualizada e suportada pelo fabricante durante toda a vigência contratual, incluindo o fornecimento de novas versões, correções, atualizações de segurança e assinaturas necessárias ao seu pleno funcionamento.

1.11. Salvo disposição expressa em contrário, as especificações constantes deste Termo de Referência representam requisitos mínimos e obrigatórios para a execução contratual.

2. CENTRO DE OPERAÇÕES DE SEGURANÇA DA INFORMAÇÃO (SOC)

2.1. A CONTRATADA deverá prover, manter e operar um Centro de Operações de Segurança (Security Operations Center - SOC) especializado na prestação dos serviços, disponibilizando toda a infraestrutura, ferramentas, processos, procedimentos e equipe técnica necessários à execução dos serviços contratados.

2.2. O SOC deverá operar de forma ininterrupta, em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano (24x7x365), durante toda a vigência contratual, assegurando a capacidade de monitoramento contínuo, detecção, investigação, resposta a incidentes, comunicação, escalonamento e suporte às atividades de contenção e mitigação de incidentes de segurança cibernética.

2.3. A CONTRATADA deverá operar o Centro de Operações de Segurança (SOC) em instalações e ambiente operacional compatíveis com a criticidade dos serviços contratados, observando requisitos de segurança física e lógica, controle de acesso, segregação de redes, disponibilidade de infraestrutura, recursos de monitoramento, canais de comunicação e processos de gestão de serviços alinhados às boas práticas de ITIL e de segurança da informação.

2.4. A CONTRATADA deverá assegurar a segurança, a disponibilidade e a continuidade dos serviços prestados pelo SOC, o qual deverá estar instalado em infraestrutura física que atenda, no mínimo, aos seguintes requisitos:

a) perímetro físico protegido por mecanismos de controle e detecção de intrusão, incluindo sensores, alarmes ou recursos equivalentes destinados à prevenção e identificação de acessos não autorizados;

b) sistema de circuito fechado de televisão (CFTV), com monitoramento e retenção das imagens gravadas por período mínimo de 90 (noventa) dias;

c) controle de acesso físico baseado em, no mínimo, dois fatores de autenticação, com registro individualizado de entradas e saídas, mantido por período mínimo de 90 (noventa) dias;

d) sistema de fornecimento ininterrupto de energia elétrica (UPS) ou solução equivalente que assegure a continuidade dos serviços em caso de interrupção do fornecimento de energia;

e) infraestrutura de telecomunicações com componentes e circuitos redundantes, compatíveis com os requisitos de disponibilidade dos serviços;

f) redes logicamente segregadas e mecanismos de controle de acesso baseados em autenticação individualizada e múltiplos fatores de autenticação;

g) proteção física das áreas operacionais de forma a impedir a visualização, captura ou acesso não autorizado às informações exibidas em telas, painéis ou estações de trabalho a partir de áreas externas ou não autorizadas.

2.5. Os mesmos controles de segurança física, lógica e administrativa exigidos para o ambiente operacional do SOC deverão ser adotados, no que couber, em qualquer ambiente utilizado na execução dos serviços, inclusive em regime de trabalho remoto. É vedado o acesso, processamento, armazenamento, transmissão ou tratamento de dados e informações do

BDMG em ambientes que não possuam nível de proteção equivalente ao exigido neste contrato e que não tenham sido previamente comunicados e formalmente aprovados pelo Banco.

2.6. O BDMG poderá realizar diligência, presencial ou remota, no ambiente de SOC da CONTRATADA a qualquer tempo durante a vigência contratual, bem como solicitar certificações e relatórios de auditoria independente relativos aos controles de segurança empregados.

2.7. A execução dos serviços observará as melhores práticas e os referenciais normativos amplamente reconhecidos no mercado de segurança da informação e segurança cibernética, incluindo, quando aplicáveis, as normas ISO/IEC 27001, ISO/IEC 27701 e ISO/IEC 27035, o NIST Cybersecurity Framework (CSF), o NIST SP 800-61, o MITRE ATT&CK, os controles e guias do SANS Institute, as metodologias e referências da OWASP, bem como outros frameworks e padrões correlatos. Tais referenciais deverão ser observados sem prejuízo do cumprimento das políticas, normas e procedimentos internos do BDMG e das disposições legais, regulatórias e normativas aplicáveis ao setor financeiro, especialmente as Resoluções CMN nº 4.893/2021 e 5.274/2025 e demais normativos que venham a complementá-las ou substituí-las.

2.8. A CONTRATADA manterá Plano de Continuidade do SOC, apresentado com o Plano de Implantação e aprovado pelo BDMG até a emissão do Termo de Recebimento Definitivo (TRD), contendo, no mínimo:

a) localidade alternativa ou operação distribuída, de modo que o SOC não dependa de instalação física única;

b) cenários de falha cobertos, incluindo a indisponibilidade de instalações, energia, telecomunicações, ferramentas da CONTRATADA e equipe;

c) procedimentos de acionamento, de comunicação ao BDMG e de retorno à operação normal;

d) responsáveis pela execução do plano.

2.9. Diante de falha que afete a operação do SOC, a CONTRATADA retomará a capacidade de monitoramento e de resposta em até 30 (trinta) minutos e comunicará o acionamento do plano ao BDMG em até 15 (quinze) minutos, com registro na ferramenta de ITSM. O acionamento do plano não suspende os prazos dos níveis de serviço, na forma do subitem 12.9.

2.10. O plano será testado, no mínimo, 1 (uma) vez por ano, em data informada previamente ao BDMG, com entrega de relatório contendo o tempo de retomada medido, as falhas encontradas e o plano de ação.

2.11. Para o indicador de Disponibilidade do SOC do subitem 12.15, considera-se indisponibilidade o período em que a CONTRATADA não mantiver capacidade efetiva de monitoramento e de resposta, caracterizado, entre outros, por:

a) ausência do contingente mínimo em atendimento efetivo no turno, na forma do subitem 7.8;

b) indisponibilidade simultânea dos canais de atendimento do subitem 8.7;

c) interrupção, sob responsabilidade da CONTRATADA, da integração entre o Microsoft Sentinel e a ferramenta de ITSM.

3. SERVIÇO GERENCIADO DE DETECÇÃO E RESPOSTA A INCIDENTES CIBERNÉTICOS (MDR)

3.1. Monitoramento e Detecção de Incidentes

3.1.1. Monitorar continuamente os eventos, alertas e incidentes de segurança gerados por ativos de infraestrutura, aplicações, sistemas corporativos, serviços e soluções de segurança do BDMG, garantindo cobertura ininterrupta 24x7x365 do ambiente monitorado.

3.1.2. Operar, analisar e tratar os incidentes, alertas e demais registros gerados pelo Microsoft Sentinel e pelas demais soluções de segurança existentes ou que venham a ser adotadas pelo BDMG, atuando diretamente no ambiente tecnológico do Banco, sem a replicação ou transferência de dados para plataformas proprietárias da CONTRATADA, salvo mediante autorização formal e expressa do BDMG.

3.1.3. Executar de forma contínua os processos de detecção, investigação, triagem, classificação, priorização, contenção, resposta e acompanhamento dos incidentes de segurança identificados.

3.1.4. Realizar análises técnicas de ameaças, indicadores de comprometimento (IOCs), endereços IP, domínios, artefatos maliciosos, logs, tráfego e registros de rede, visando identificar atividades suspeitas ou comprometimentos do ambiente.

3.1.5. Consolidar, por meio do Microsoft Sentinel, a visão centralizada de incidentes, riscos e prioridades de tratamento, promovendo sua integração com a solução de gestão de vulnerabilidades mediante conectores nativos ou, quando indisponíveis, por APIs, webhooks ou playbooks desenvolvidos pela CONTRATADA, sem custos adicionais para o BDMG.

3.1.6. Monitorar continuamente fontes internas e externas de inteligência de ameaças, incluindo comunidades especializadas, fornecedores e agências de inteligência cibernética, incorporando informações relevantes aos processos de detecção e resposta.

3.1.7. Verificar a aderência do ambiente às políticas, normas, padrões e requisitos regulatórios aplicáveis, reportando desvios identificados e recomendando as medidas corretivas necessárias.

3.1.8. Avaliar os riscos associados aos achados oriundos dos serviços de Caça a Ameaças (Threat Hunting) e de Gestão de Vulnerabilidades, classificando-os de acordo com critérios de criticidade, impacto potencial ao negócio e probabilidade de exploração.

3.1.9. Elaborar recomendações técnicas detalhadas para o fortalecimento da postura de segurança do BDMG, contemplando correções, atualizações, ajustes de configuração, aperfeiçoamento de controles, definição de políticas e demais medidas de mitigação.

3.1.10. Registrar e acompanhar as requisições de serviço necessárias à implementação das ações corretivas e mitigatórias recomendadas, validando sua execução e efetividade.

INFORMAÇÃO CONTROLADA

3.1.11. Atuar de forma integrada com o serviço de Caça a Ameaças (Threat Hunting) e com a equipe de segurança do BDMG, visando identificar fragilidades, validar a eficácia dos controles existentes e recomendar melhorias contínuas dos mecanismos de proteção.

3.1.12. Exercer papel central na condução e coordenação da resposta a incidentes classificados como médios, altos, críticos ou caracterizados como crises cibernéticas.

3.1.13. Realizar, quando aplicável e mediante autorização prévia do BDMG, a reconstrução controlada de ataques relacionados a incidentes que envolvam comprometimento, fraude ou vazamento de informações, em ambiente segregado e seguro, próprio ou contratado pela CONTRATADA, sendo vedada a utilização de dados pessoais, sigilosos ou sensíveis do BDMG sem os devidos processos de anonimização. Ao término da análise, deverá ser comprovada a eliminação dos artefatos utilizados.

3.1.14. Documentar, consolidar e manter atualizada, durante toda a vigência contratual, uma base de conhecimento contendo lições aprendidas, indicadores observados, técnicas utilizadas por agentes maliciosos, ações executadas e recomendações decorrentes dos incidentes tratados, contribuindo para o aprimoramento contínuo da capacidade de detecção e resposta do BDMG.

3.2. Resposta a Incidentes

3.2.1. Iniciar o processo de resposta a incidentes imediatamente após o reporte de um evento adverso pelo SIEM ou por outras fontes de detecção autorizadas.

3.2.2. Analisar logs, eventos e demais artefatos disponíveis, com o objetivo de identificar as origens e os ativos responsáveis pela geração dos eventos reportados.

3.2.3. Identificar e avaliar os vetores de ataque utilizados no comprometimento do ambiente do BDMG.

3.2.4. Comunicar à equipe de segurança cibernética do BDMG as informações preliminares relacionadas ao incidente, incluindo a avaliação inicial do impacto e as estratégias previstas para tratamento e resolução.

3.2.5. Registrar, de forma detalhada, a prioridade, classificação, origem, destino, fontes de detecção, ações recomendadas e demais informações relevantes relativas ao incidente.

3.2.6. Determinar a severidade do incidente em conjunto com o BDMG, considerando critérios de impacto ao negócio, urgência e potencial risco ao ambiente.

3.2.7. Realizar análise aprofundada do comportamento do ataque, ameaça ou artefato malicioso, visando identificar sua abrangência, impacto e mecanismos de atuação.

3.2.8. Definir e implementar estratégias de mitigação e contenção, mediante autorização prévia do BDMG para alterações no ambiente. Em situações críticas que exijam ações imediatas de contenção fora do horário de expediente, a preservação da segurança do ambiente deverá prevalecer, com posterior comunicação ao BDMG.

3.2.9. Executar, mediante prévia autorização do BDMG, as ações de contenção, mitigação e remediação de incidentes de segurança da informação, incluindo entre outras, quando aplicável:

3.2.9.1. isolamento de estações de trabalho, servidores ou outros ativos;
3.2.9.2. bloqueio de endereços IP, domínios, URLs ou indicadores maliciosos;
3.2.9.3. bloqueio ou encerramento de processos suspeitos;
3.2.9.4. remoção de arquivos maliciosos identificados;
3.2.9.5. desativação ou bloqueio temporário de contas comprometidas;
3.2.9.6. revogação de sessões ativas;
3.2.9.7. bloqueio de credenciais comprometidas;
3.2.9.8. restrição de comunicação entre ativos afetados.

3.2.10. Coletar e preservar evidências, identificar os serviços afetados e conduzir análises forenses necessárias para apuração do incidente.

3.2.11. Apoiar a restauração dos serviços afetados, atuando em conjunto com as equipes de Segurança e Tecnologia do BDMG.

3.2.12. Consolidar as evidências coletadas, correlacionar as informações apuradas e elaborar relatório ou laudo conclusivo do incidente, quando aplicável.

3.2.13. Em caso de incidentes cibernéticos relevantes, a CONTRATADA deverá colaborar, mediante autorização prévia do BDMG e observadas as regras aplicáveis de confidencialidade, com equipes internas e externas de resposta a incidentes, incluindo CSIRTs, CERTs e o CTIR Gov. A CONTRATADA também prestará apoio técnico ao BDMG nas comunicações destinadas a órgãos reguladores e à ANPD, sem quaisquer custos adicionais.

3.2.14. Desenvolver, no prazo máximo de 48 (quarenta e oito) horas após o encerramento do tratamento do incidente, um caso de uso de detecção compatível com o evento tratado, anexando todas as evidências necessárias para sua adequada conclusão e encerramento.

3.3. Sala de Guerra (War Room)

3.3.1. A CONTRATADA deverá disponibilizar e operar Sala de Guerra para tratamento de incidentes classificados como críticos (P1) e sempre que solicitado pelo BDMG.

3.3.2. A Sala de Guerra deverá ser estabelecida em até 30 (trinta) minutos após seu acionamento, com a participação mínima de profissional da CONTRATADA responsável por liderar e coordenar a resposta a um incidente (Incident Commander) e de analista especializado responsável pelo tratamento do incidente.

3.3.3. A operação deverá ocorrer em ambiente virtual colaborativo disponibilizado ou aprovado pelo BDMG.

3.3.4. A CONTRATADA deverá manter equipe técnica qualificada e com autoridade para coordenar ações de investigação, contenção, erradicação, recuperação e comunicação durante todo o ciclo de tratamento do incidente.

INFORMAÇÃO CONTROLADA

3.3.5. Quando houver envolvimento de fornecedores, fabricantes, prestadores de serviços ou provedores de nuvem, a CONTRATADA deverá coordenar tecnicamente as interações necessárias à resolução do incidente, em conjunto com o BDMG.

3.3.6. A Sala de Guerra deverá operar em regime contínuo enquanto persistir a necessidade de tratamento do incidente, mantendo registro atualizado das atividades executadas, decisões tomadas, evidências coletadas e responsáveis envolvidos.

3.3.7. A CONTRATADA deverá fornecer atualizações periódicas de status, em frequência compatível com a criticidade do incidente, até sua contenção e normalização.

3.3.8. Após o encerramento do incidente, a CONTRATADA deverá elaborar relatório de lições aprendidas contendo, no mínimo, cronologia do evento, causa raiz, ações executadas, impactos observados, oportunidades de melhoria e plano de ação para prevenção de recorrência.

3.3.9. As lições aprendidas deverão ser utilizadas para aprimorar os casos de uso de detecção, playbooks de resposta, hipóteses de caça a ameaças, processos operacionais e demais controles de segurança relacionados.

3.3.10. Todos os custos da CONTRATADA relacionados ao acionamento e à operação da Sala de Guerra, incluindo mobilização de equipes, participação de especialistas, reuniões e elaboração de relatórios, deverão estar incluídos no valor contratual.

3.3.11. A CONTRATADA deverá realizar em conjunto com o BDMG, no mínimo, 1 (um) exercício anual de simulação de incidente crítico com acionamento da Sala de Guerra, apresentando relatório com os resultados e oportunidades de melhoria identificadas.

3.4. Caça a Ameaças (Threat Hunting)

3.4.1. O Serviço de Caça a Ameaças (Threat Hunting) consiste na identificação proativa, contínua e orientada por hipóteses de ameaças, comportamentos maliciosos, indicadores de comprometimento (IOCs) e técnicas adversárias eventualmente não detectados pelos mecanismos convencionais de monitoramento e detecção. O serviço deverá ser executado utilizando o Microsoft Sentinel e as demais fontes de telemetria disponíveis no ambiente do BDMG, com o objetivo de reduzir o tempo de permanência de ameaças no ambiente e aprimorar continuamente a capacidade de detecção e resposta do Banco.

3.4.2. O serviço deverá integrar a operação regular do SOC/MDR, sendo executado de forma contínua, independentemente de acionamento prévio pelo BDMG.

3.4.3. As atividades de caça a ameaças deverão ser baseadas, no mínimo, em:

a) técnicas e subtécnicas do framework MITRE ATT&CK;

b) informações de inteligência de ameaças;

c) indicadores de comprometimento (IOCs);

d) táticas, técnicas e procedimentos (TTPs) relevantes ao setor financeiro;

e) vulnerabilidades críticas identificadas no ambiente;

INFORMAÇÃO CONTROLADA

f) incidentes de segurança previamente tratados;

g) hipóteses definidas pela CONTRATADA ou pelo BDMG.

3.4.4. A CONTRATADA deverá executar, no mínimo, 1 (uma) campanha estruturada de Threat Hunting por mês, devendo apresentar ao BDMG o planejamento trimestral das campanhas a serem realizadas.

3.4.5. Além das campanhas programadas, a CONTRATADA deverá executar campanhas extraordinárias sempre que houver:

a) identificação de novas ameaças relevantes ao ambiente ou ao setor financeiro;

b) ocorrência de incidentes críticos ou de alta severidade;

c) divulgação de vulnerabilidades críticas com exploração ativa;

d) solicitação do BDMG.

3.4.6. Cada campanha deverá gerar relatório contendo, no mínimo:

a) hipótese investigada;

b) escopo analisado;

c) fontes de dados utilizadas;

d) consultas realizadas;

e) evidências coletadas;

f) achados identificados;

g) conclusões e recomendações.

3.4.7. Os resultados das campanhas deverão ser utilizados para aprimorar continuamente os mecanismos de monitoramento e detecção, por meio da criação ou atualização de:

a) regras analíticas;

b) consultas de investigação;

c) casos de uso;

d) playbooks;

e) automações;

f) requisitos de novas fontes de telemetria.

3.4.8. Sempre que uma atividade de Threat Hunting identificar indícios de comprometimento ou incidente de segurança, a CONTRATADA deverá iniciar imediatamente o processo de tratamento de incidente previsto neste Termo de Referência.

3.4.8-A. A CONTRATADA apurará, por trimestre, a Taxa de Incidentes Iniciados por Caça a Ameaças (HIIRR – Hunt-Initiated Incident Response Rate). O HIIRR corresponde ao percentual de incidentes confirmados como verdadeiro positivo no trimestre que foram

descobertos por campanha de Caça a Ameaças, sem alerta prévio de regra analítica sobre a mesma atividade. A meta é de, no mínimo, 25% (vinte e cinco por cento), e o resultado constará do relatório trimestral do subitem 3.4.9.

3.4.8-B. Somente será computado o incidente vinculado, no chamado, à campanha que o originou e registrado no relatório da campanha, na forma do subitem 3.4.6. A origem do incidente está sujeita à auditoria de Acurácia de Classificação do subitem 12.17, vedada a reclassificação de incidente originado por alerta. Por depender também da atuação de agentes de ameaça no ambiente, o HIIRR é indicador de acompanhamento, não sujeito às glosas do subitem 12.25. O não atingimento da meta em 2 (dois) trimestres consecutivos ensejará análise de causa raiz e plano de ação, na forma do subitem 11.17.

3.4.9. A CONTRATADA deverá apresentar relatório trimestral consolidado contendo:

a) campanhas realizadas;

b) principais achados;

c) evolução da cobertura MITRE ATT&CK;

d) novos casos de uso implementados;

e) lacunas de visibilidade identificadas;

f) plano de trabalho para o trimestre subsequente.

3.4.10. Todas as evidências, consultas, relatórios, indicadores, regras e demais artefatos produzidos deverão ser registrados e permanecerão como propriedade exclusiva do Banco.

3.4.11. O serviço possui caráter exclusivamente defensivo e investigativo, sendo vedada a execução de atividades ofensivas, exploração de vulnerabilidades, alterações em ambientes produtivos ou quaisquer ações que possam impactar a disponibilidade, integridade ou confidencialidade dos ativos sem autorização formal do BDMG.

3.5. Engenharia de Detecção e Otimização do SIEM Microsoft Sentinel

3.5.1. O Serviço de Engenharia de Detecção (Detection Engineering) tem por objetivo projetar, desenvolver, implementar, testar, manter e evoluir continuamente as capacidades de detecção de ameaças cibernéticas do BDMG, adotando os princípios de Detection as Code (DaC), de forma a garantir rastreabilidade, padronização, governança, versionamento e melhoria contínua dos mecanismos de monitoramento e resposta.

3.5.2. As atividades serão executadas pela CONTRATADA utilizando, prioritariamente, os recursos nativos do Microsoft Sentinel, incluindo regras analíticas, consultas KQL (Kusto Query Language), Hunting Queries, Workbooks, Automation Rules, Playbooks, Watchlists, Threat Intelligence, UEBA e demais funcionalidades disponíveis ou que venham a ser disponibilizadas pela plataforma durante a vigência contratual.

3.5.3. A CONTRATADA deverá transformar informações provenientes de inteligência de ameaças, incidentes de segurança, campanhas de Caça a Ameaças (Threat Hunting),

vulnerabilidades identificadas e análises do ambiente em regras analíticas, consultas, correlações, automações, playbooks e casos de uso implementados no Microsoft Sentinel, ampliando a capacidade de detecção de comportamentos maliciosos e reduzindo o tempo de identificação e resposta a incidentes.

3.5.4. A CONTRATADA deverá manter processo contínuo de pesquisa e análise de ameaças com o objetivo de identificar técnicas, táticas, procedimentos e comportamentos utilizados por agentes maliciosos relevantes ao ambiente do BDMG. As atividades de pesquisa deverão considerar, no mínimo:

a) a matriz MITRE ATT&CK e suas respectivas táticas, técnicas e subtécnicas;
b) indicadores de comprometimento (IOCs);
c) indicadores de comportamento (IOBs);
d) relatórios de inteligência de ameaças;
e) campanhas e grupos criminosos relevantes para o setor financeiro;
f) vulnerabilidades críticas identificadas no ambiente;
g) incidentes tratados pelo SOC;
h) resultados das campanhas de Threat Hunting;
i) requisitos e hipóteses formuladas pelo BDMG;
j) recomendações decorrentes de auditorias, testes de segurança e exercícios de resposta a incidentes.

3.5.5. A CONTRATADA deverá manter mapeamento das capacidades de detecção implementadas em relação ao framework MITRE ATT&CK, identificando periodicamente lacunas de cobertura e propondo ações para sua mitigação.

3.5.6. A CONTRATADA deverá projetar, desenvolver, implementar, documentar, revisar e manter regras analíticas, consultas KQL, mecanismos de correlação, casos de uso, conteúdos de detecção, automações e playbooks no Microsoft Sentinel.

3.5.7. As detecções deverão contemplar eventos e correlações provenientes das diversas fontes de dados integradas ao ambiente de monitoramento do BDMG, incluindo identidades, endpoints, servidores, aplicações, serviços em nuvem, dispositivos de rede e demais ativos monitorados.

3.5.8. As regras e casos de uso deverão ser desenvolvidos considerando diferentes cenários de ataque, movimentação lateral, escalonamento de privilégios, persistência, exfiltração de dados, evasão de defesa, comprometimento de credenciais, atividades anômalas e demais comportamentos relevantes à segurança cibernética.

3.5.9. A CONTRATADA deverá adotar práticas de Detection as Code, com versionamento em repositório Git indicado pelo BDMG, assegurando que todas as regras, consultas, automações e artefatos de detecção sejam:

a) documentados;
b) versionados;
c) rastreáveis e auditáveis;
d) submetidos a processo formal de homologação e controle de mudanças;

e) armazenados em repositório definido pelo BDMG;
f) possuam histórico de alterações e responsáveis pelas modificações realizadas;
g) mantidos em repositório Git indicado pelo BDMG, em formatos abertos e legíveis por máquina, com portabilidade assegurada e sem dependência de ferramenta proprietária da CONTRATADA;
h) submetidos a revisão formal por pares antes da publicação em produção, mediante mecanismo de solicitação de alteração (pull request ou equivalente) com aprovador identificado, vedada a publicação direta sem revisão registrada;
i) submetidos a testes documentados antes da promoção a produção, contemplando validação de sintaxe, de lógica de detecção e de ausência de degradação de desempenho ou de elevação indevida de falsos positivos;
j) dotados de procedimento de retorno à versão anterior (rollback) documentado, testado e executável, com registro do responsável, da motivação e do horário da reversão.

3.5.10. Toda nova detecção implementada deverá possuir documentação mínima contendo objetivo, lógica empregada, fontes de dados utilizadas, requisitos, cobertura MITRE ATT&CK, tratamento esperado e critério de severidade.

3.5.11. A CONTRATADA deverá assegurar a qualidade, disponibilidade, integridade e adequação das fontes de dados utilizadas nos processos de monitoramento, investigação e detecção. Para esse fim, deverá:

a) avaliar periodicamente as fontes de telemetria integradas ao Microsoft Sentinel;
b) verificar a correta configuração da coleta de logs e eventos dos ativos monitorados;
c) validar a integridade, completude e consistência dos dados ingeridos;
d) monitorar falhas de coleta, perdas de eventos, duplicidades e degradações de qualidade dos dados;
e) identificar lacunas de visibilidade que possam comprometer a capacidade de detecção.

3.5.12. A CONTRATADA deverá recomendar a inclusão de novas fontes de dados, eventos, campos de telemetria ou mecanismos de auditoria sempre que necessário para ampliar a cobertura de monitoramento e detecção.

3.5.13. Também deverá implementar e manter processos de normalização, enriquecimento, classificação e padronização dos dados de segurança, garantindo seu correto aproveitamento pelas capacidades de correlação, investigação, análise comportamental e detecção implementadas no Microsoft Sentinel.

3.5.14. Sempre que identificadas limitações ou deficiências de telemetria, a CONTRATADA deverá registrar a ocorrência, avaliar seu impacto na cobertura de detecção e apresentar recomendação formal de mitigação ao BDMG.

3.5.15. A CONTRATADA deverá manter processo permanente de validação técnica, testes, calibração e aprimoramento das regras e mecanismos de detecção implementados.

INFORMAÇÃO CONTROLADA

3.5.16. As detecções deverão ser submetidas a testes periódicos em ambiente controlado ou por meio de técnicas de emulação de adversários, visando validar sua capacidade de identificar comportamentos maliciosos representativos de ameaças reais.

3.5.17. A CONTRATADA deverá realizar atividades contínuas de calibração (tuning), com objetivo de:

a) reduzir a ocorrência de falsos positivos;
b) minimizar falsos negativos;
c) aumentar a precisão dos alertas;
d) reduzir a fadiga operacional da equipe de monitoramento;
e) melhorar a eficiência dos processos de investigação.

3.5.18. Os resultados obtidos em incidentes reais, campanhas de Threat Hunting, simulações, testes de segurança, análises de ameaças e exercícios de resposta deverão ser utilizados para revisão e aprimoramento contínuo das capacidades de detecção do SIEM.

3.5.19. Sempre que identificadas lacunas de cobertura ou oportunidades de melhoria, a CONTRATADA deverá criar ou revisar regras analíticas, consultas, automações, correlações, playbooks e demais mecanismos de detecção.

3.5.20. O Serviço de Engenharia de Detecção atuará de forma integrada aos serviços de:

a) Monitoramento e Correlação de Eventos;
b) Resposta a Incidentes;
c) Threat Hunting;
d) Gestão de Vulnerabilidades;
e) Inteligência de Ameaças (Threat Intelligence), na forma do item 3.7.

3.5.21. Os resultados produzidos por qualquer uma dessas disciplinas deverão ser avaliados quanto à necessidade de criação, atualização ou aperfeiçoamento de mecanismos de detecção no Microsoft Sentinel.

3.5.22. A CONTRATADA deverá acompanhar e apresentar indicadores de desempenho relacionados à capacidade de detecção, incluindo, no mínimo:

a) cobertura MITRE ATT&CK;
b) quantidade de casos de uso implementados e revisados;
c) quantidade de regras e correlações implantadas;
d) taxa de falsos positivos;
e) eficiência das detecções implementadas;
f) lacunas de cobertura identificadas;
g) evolução da maturidade da capacidade de detecção.

3.5.23. A CONTRATADA deverá apresentar relatório trimestral contendo, no mínimo:

a) novas detecções implementadas;
b) detecções revisadas ou descontinuadas;

INFORMAÇÃO CONTROLADA

c) cobertura MITRE ATT&CK atualizada;
d) melhorias realizadas;
e) resultados dos testes e calibrações;
f) lacunas identificadas;
g) plano de evolução da capacidade de detecção para o período subsequente.

3.5.23-A. A CONTRATADA apurará, por trimestre, o Rendimento da Engenharia de Detecção (DEY – Detection Engineering Yield), que corresponde à quantidade de novas detecções particularizadas promovidas a produção no Microsoft Sentinel do BDMG no trimestre. A meta é de, no mínimo, 6 (seis) novas detecções particularizadas por trimestre, priorizadas pelas lacunas do subitem 3.5.5 e pela modelagem de ameaças do subitem 3.7.6. O relatório do subitem 3.5.23 apresentará o DEY e a variação da cobertura MITRE ATT&CK, com as técnicas e subtécnicas cobertas no início e no fim do trimestre.

3.5.23-B. Considera-se detecção particularizada a regra analítica desenvolvida ou adaptada para o ambiente do BDMG, versionada na forma do subitem 3.5.9, documentada na forma do subitem 3.5.10 e mapeada a, no mínimo, 1 (uma) técnica ou subtécnica do MITRE ATT&CK. Não serão computados:

a) modelos (templates) nativos do Microsoft Sentinel ativados sem adaptação;

b) simples ajustes de limiar ou de exclusões em regra existente;

c) regras desativadas em até 30 (trinta) dias da publicação por excesso de falsos positivos.

3.5.24. Todas as regras, consultas, casos de uso, playbooks, automações, correlações, documentações, relatórios e demais artefatos produzidos no âmbito deste serviço serão de propriedade exclusiva do BDMG.

3.5.25. Os artefatos deverão permanecer armazenados em ambiente indicado pelo BDMG, vedada sua retenção exclusiva em ambiente da CONTRATADA.

3.5.26. A CONTRATADA manterá o volume de ingestão de dados no Microsoft Sentinel do BDMG dentro da linha de base de referência indicada no subitem 6.1, competindo-lhe submeter previamente ao Banco, com justificativa técnica, estimativa de impacto e alternativas de otimização, qualquer alteração de configuração, inclusão de fonte, ampliação de escopo de coleta ou mudança de regra de transformação que eleve o volume ingerido acima dessa linha de base. Ressalvam-se da exigência de submissão prévia as elevações decorrentes de incidente de segurança em curso, de determinação do BDMG ou de fato alheio à gestão da CONTRATADA, que serão comunicadas ao Banco em até 1 (um) dia útil, com a respectiva justificativa.

3.5.27. A CONTRATADA reportará mensalmente o volume ingerido e o custo estimado por tabela e por fonte de dados, acompanhados dos dados brutos que sustentam a apuração, na forma dos subitens 11.13, alínea 'e', e 11.14, e apresentará trimestralmente plano de otimização do custo de ingestão, com oportunidades quantificadas, economias realizadas no período e recomendações para o trimestre subsequente.

INFORMAÇÃO CONTROLADA

3.6. A CONTRATADA deverá compartilhar periodicamente com o BDMG informações relevantes obtidas em comunidades, fóruns e redes especializadas em segurança cibernética, especialmente aquelas relacionadas ao setor financeiro, que possam contribuir para a prevenção, detecção e resposta a ameaças cibernéticas.

3.7. **Inteligência de Ameaças (Threat Intelligence)**

3.7.1. O Serviço de Inteligência de Ameaças (Threat Intelligence) consiste na coleta, integração, curadoria, análise, enriquecimento, produção e disseminação de inteligência sobre ameaças cibernéticas relevantes ao ambiente do BDMG e ao setor financeiro, com o objetivo de antecipar cenários de ataque, orientar as hipóteses de Caça a Ameaças, qualificar a severidade das detecções e dos incidentes e subsidiar as decisões de priorização de risco do Banco.

3.7.2. O serviço integra o Serviço Gerenciado de Detecção e Resposta a Incidentes Cibernéticos (MDR), item 1 do quadro de itens do subitem 1.1, não constituindo item, parcela ou valor destacado na planilha de preços, e será executado de forma contínua, independentemente de acionamento prévio pelo BDMG.

3.7.3. A CONTRATADA manterá equipe própria de Inteligência de Ameaças, funcionalmente distinta da equipe de Caça a Ameaças (Threat Hunting) e da equipe de monitoramento (N1, N2 e N3), sendo vedado que a disciplina de Inteligência de Ameaças seja exercida como atividade residual dos analistas de plantão ou substituída pelo simples consumo de feeds automatizados. O profissional designado observará os requisitos do subitem 7.17.

3.7.4. Compete à CONTRATADA integrar, curar e enriquecer feeds de inteligência de ameaças, próprios e de terceiros, nos padrões STIX (Structured Threat Information Expression) e TAXII (Trusted Automated Exchange of Intelligence Information), inclusive mediante conexão aos recursos nativos de Threat Intelligence do Microsoft Sentinel do BDMG, sem qualquer custo adicional de ferramenta, plataforma, assinatura, feed ou licença para o Banco, cujos custos se consideram integralmente incluídos no preço mensal do item 1 do quadro de itens.

3.7.5. A CONTRATADA realizará análise periódica do cenário de ameaças (Threat Landscape) aplicável ao BDMG e ao setor financeiro brasileiro, contemplando ameaças emergentes, campanhas em curso, vulnerabilidades com exploração ativa, tendências de fraude eletrônica e riscos associados ao ambiente do Sistema de Pagamentos Brasileiro a que se refere o subitem 6.3.

3.7.6. A CONTRATADA manterá mapeamento de agentes de ameaça (Threat Actors) relevantes ao BDMG e desenvolverá perfis de ameaça e modelagem de ameaças (Threat Modeling) sobre os ativos, serviços e fluxos críticos do Banco, utilizando como referência, no mínimo, o framework MITRE ATT&CK e a metodologia STRIDE, ou referências equivalentes previamente aprovadas pelo BDMG, indicando, para cada agente ou cenário, as táticas, técnicas e procedimentos (TTPs) associados, a cobertura de detecção existente no Microsoft Sentinel e as lacunas identificadas.

3.7.7. A CONTRATADA executará a análise e a gestão do ciclo de vida dos indicadores de comprometimento (IoCs), compreendendo a coleta, a validação, a classificação por confiabilidade e relevância, o enriquecimento contextual, a inserção nos mecanismos de detecção e de bloqueio do ambiente do BDMG, o acompanhamento da respectiva eficácia e a expiração ou o descarte dos indicadores obsoletos, de modo a evitar a degradação da qualidade das detecções e o aumento de falsos positivos.

3.7.8. Os produtos de inteligência serão compartilhados de forma estruturada com a equipe de Caça a Ameaças (Threat Hunting), para formulação das hipóteses de caça de que trata o subitem 3.4.3, e com o Serviço de Engenharia de Detecção, para conversão em regras analíticas, consultas e casos de uso, na forma do subitem 3.5.3. Todo IoC classificado como crítico, e todo relatório de inteligência que identifique ameaça com exploração ativa relevante ao ambiente do Banco, gerará obrigatoriamente, e sem custo adicional, hipótese formal de caça a ameaças ou ajuste de detecção, registrados em chamado e concluídos em até 48 (quarenta e oito) horas contadas da respectiva identificação.

3.7.9. A disciplina de Inteligência de Ameaças não substitui nem se confunde com a Caça a Ameaças (Threat Hunting): a primeira produz o conhecimento sobre o adversário e o contexto externo; a segunda o aplica, de forma investigativa, sobre a telemetria do ambiente do BDMG. O descumprimento das entregas de uma disciplina não é suprido pela execução da outra.

3.7.10. A CONTRATADA entregará, no mínimo: a) boletim mensal de inteligência de ameaças, até o 5º (quinto) dia útil de cada mês, contendo o cenário do período, os agentes e as campanhas observados, os IoCs incorporados e descartados, as ameaças emergentes e as recomendações de ação; b) relatório trimestral de Threat Landscape e de modelagem de ameaças, com atualização dos perfis de agentes de ameaça, da cobertura MITRE ATT&CK associada e das lacunas identificadas; e c) alerta extraordinário de inteligência, em até 4 (quatro) horas da identificação, sempre que houver ameaça com exploração ativa, campanha dirigida ao setor financeiro ou vulnerabilidade crítica com potencial de impacto imediato ao ambiente do Banco.

3.7.11. Todos os relatórios, perfis de ameaça, modelagens, indicadores, consultas e demais artefatos produzidos no âmbito deste serviço são de propriedade exclusiva do BDMG, permanecerão armazenados em ambiente por ele indicado, na forma dos subitens 3.5.24 e 3.5.25, e serão entregues na transição contratual, na forma do item 14.1, vedada a retenção exclusiva em ambiente da CONTRATADA e vedado o condicionamento do acesso a qualquer pagamento adicional.

3.8. **Uso de Inteligência Artificial Generativa na Operação**

3.8.1. A CONTRATADA poderá empregar recursos de Inteligência Artificial Generativa como apoio às atividades de triagem, enriquecimento, correlação, sumarização e documentação de eventos e incidentes de segurança, bem como à elaboração de consultas, regras e relatórios, observadas integralmente as condições deste item.

3.8.2. A utilização de Inteligência Artificial Generativa tem caráter exclusivamente auxiliar e não transfere à ferramenta a responsabilidade técnica pela análise, pela classificação, pela decisão ou pelo resultado, que permanece integralmente da CONTRATADA e dos profissionais por ela designados.

3.8.3. É obrigatória a validação humana prévia (human-in-the-loop) por profissional qualificado da CONTRATADA antes da execução de qualquer ação em ambiente de produção do BDMG, sendo vedada a execução automática, autônoma ou não supervisionada, por recurso de Inteligência Artificial Generativa, de ações de contenção, bloqueio, isolamento, desativação de contas, alteração de configuração, encerramento de incidentes ou de chamados e quaisquer outras providências com efeito sobre o ambiente, sobre a medição dos níveis de serviço ou sobre a apuração de glosas.

3.8.4. A utilização de recursos de Inteligência Artificial Generativa que processem dados do BDMG dependerá de comunicação prévia e de aprovação formal do Banco, com identificação da ferramenta, do fornecedor, da finalidade, dos dados processados, do país de processamento e armazenamento e das salvaguardas adotadas, observadas as condições de localização de dados, de confidencialidade e de tratamento de dados pessoais estabelecidas no instrumento contratual.

3.8.5. É vedada a utilização de dados, logs, evidências, artefatos, regras, indicadores ou quaisquer informações do BDMG para treinamento, ajuste fino, avaliação ou aperfeiçoamento de modelos de Inteligência Artificial, próprios ou de terceiros, ainda que sob a forma de dados agregados, anonimizados ou de inteligência de ameaças, salvo autorização prévia, expressa e específica do Banco.

3.8.6. A CONTRATADA manterá registro auditável da utilização de Inteligência Artificial Generativa nas atividades contratadas, identificando, no mínimo, os incidentes e chamados em que houve apoio da ferramenta, a natureza do apoio prestado e o profissional responsável pela validação humana, e disponibilizará esse registro ao BDMG mediante solicitação e nas reuniões de governança.

3.8.7. O emprego de Inteligência Artificial Generativa não reduz, flexibiliza nem substitui os quantitativos mínimos de equipe do item 7, os requisitos de qualificação técnica dos profissionais, os níveis mínimos de serviço do item 12 ou qualquer outra obrigação contratual, e não constitui fundamento para recusa, postergação ou reclassificação de atendimento.

3.9. **Limites de Automação e Ações de Alto Risco**

3.9.1. A CONTRATADA poderá executar contenção automática, sem aprovação humana caso a caso, somente quando atendidas, ao mesmo tempo, as seguintes condições:

a) a ação constar de playbook aprovado previamente pelo BDMG, versionado e testado na forma do subitem 3.5.9;

b) o alerta tiver nível de confiança igual ou superior a 95% (noventa e cinco por cento), na forma do subitem 3.9.2;

INFORMAÇÃO CONTROLADA

c) a ação for reversível e de baixo impacto, limitada a isolamento (quarentena) de estação de trabalho ou de servidor não crítico, bloqueio de endereço IP, domínio, URL ou hash malicioso, encerramento de processo malicioso e revogação de sessões ativas de conta não privilegiada;

d) o ativo, a conta ou o endereço não constar da Lista de Ativos Críticos nem da lista de exceções mantida pelo BDMG, nem integrar o ambiente de participação do BDMG no Sistema de Pagamentos Brasileiro (SPB), de que trata o subitem 6.3.

3.9.2. O nível de confiança corresponde:

a) para regra analítica, ao percentual de incidentes por ela gerados e confirmados como verdadeiro positivo nos últimos 90 (noventa) dias, apurado sobre, no mínimo, 20 (vinte) incidentes;

b) para indicador de comprometimento (IoC), ao grau de confiança registrado na Inteligência de Ameaças do Microsoft Sentinel do BDMG, após a curadoria do subitem 3.7.7.

3.9.3. A aprovação do playbook pelo BDMG constitui a autorização prévia de que tratam os subitens 3.2.8 e 3.2.9, nos limites deste item. A contenção automática será executada pela lógica determinística do playbook, vedado que a decisão de executá-la seja tomada por recurso de Inteligência Artificial Generativa, na forma do subitem 3.8.3.

3.9.4. Toda contenção automática será registrada no chamado e comunicada ao BDMG pela ferramenta de ITSM, com o playbook, a versão, a regra e o nível de confiança. A ação será submetida à triagem do analista nos prazos de MTTA do subitem 12.14 e desfeita de imediato se confirmado falso positivo.

3.9.5. Dependem de autorização expressa e nominal do BDMG, registrada no chamado, em qualquer dia e horário, as seguintes ações de alto risco, ressalvadas as previamente autorizadas na forma do subitem 3.9.6:

a) redefinição (reset) de senhas, chaves ou certificados de contas privilegiadas ou de serviço;

b) reinicialização ou desligamento de servidores, serviços ou aplicações;

c) restauração de dados ou de sistemas a partir de cópias de segurança;

d) isolamento de controlador de domínio;

e) alteração de políticas de acesso ou de identidade, ou de regras de firewall que afetem serviços em produção, exceto o bloqueio de indicador malicioso previsto no subitem 3.9.1;

f) qualquer ação sobre o ambiente do SPB;

g) ação sobre ativo da Lista de Ativos Críticos cujo regime, definido pelo BDMG, exija aprovação nominal.

3.9.6. Não se aplica às ações do subitem 3.9.5 a ressalva do subitem 3.2.8 que admite contenção imediata fora do horário de expediente, com comunicação posterior. O BDMG poderá autorizar previamente, na matriz RACI do subitem 11.17-A, ações do subitem 3.9.5 para situações nela definidas. As demais aguardarão a autorização do BDMG, aplicando-se ao período de espera o Clock Stop do subitem 12.8.

3.9.7. A CONTRATADA apurará e reportará mensalmente, como indicadores de acompanhamento, sem meta e sem glosa:

a) Taxa de Autonomia: percentual de incidentes contidos ou encerrados integralmente por automação aprovada, sem intervenção humana na execução;

b) percentual de incidentes com apoio de Inteligência Artificial Generativa, conforme o registro do subitem 3.8.6;

c) economia de tempo dos analistas, em horas, calculada pelo número de execuções de cada playbook multiplicado pelo tempo manual de referência da tarefa, declarado na documentação do playbook e aprovado pelo BDMG.

3.9.8. Os incidentes encerrados por automação integram a amostra da auditoria de Acurácia de Classificação do subitem 12.17.

4. SERVIÇO DE GESTÃO DE VULNERABILIDADES

4.1. O Serviço de Gestão de Vulnerabilidades tem por objetivo identificar, de forma contínua, proativa e recorrente, vulnerabilidades de segurança em ativos de infraestrutura de TI, sistemas operacionais, bancos de dados, dispositivos de rede e aplicações web, por meio da realização de varreduras automatizadas, análises especializadas e emissão de relatórios técnicos. Também incluirá o gerenciamento da implantação de atualizações e correções de software (patches).

4.2. O serviço deverá apoiar a redução da superfície de ataque do BDMG, prevenindo a exploração de vulnerabilidades conhecidas por agentes maliciosos. A CONTRATADA deverá, ainda, prestar suporte técnico ao BDMG na definição e implementação das medidas de correção e mitigação recomendadas, mediante a emissão de relatórios contendo a descrição das vulnerabilidades identificadas, sua criticidade, riscos associados e respectivas ações de remediação.

4.3. O serviço de Gestão de Vulnerabilidades contemplará, no mínimo, as seguintes atividades:

4.3.1. Licenciamento, implantação, configuração, operação e sustentação da solução de gerenciamento de vulnerabilidades fornecida pela CONTRATADA, incluindo integrações necessárias ao pleno funcionamento do serviço;

4.3.2. Realização periódica de varreduras de vulnerabilidades em ativos de infraestrutura de TI, sistemas operacionais, bancos de dados, dispositivos de rede, aplicações web e demais ativos incluídos no escopo pelo BDMG;

4.3.3. Análise, validação e tratamento de falsos positivos identificados nas varreduras, assegurando que apenas vulnerabilidades efetivamente confirmadas sejam reportadas ao BDMG;

INFORMAÇÃO CONTROLADA

4.3.4. Elaboração e entrega de relatórios técnicos contendo, no mínimo: a) vulnerabilidades identificadas; b) classificação de criticidade; c) ativos afetados; d) riscos associados; e) vulnerabilidades não corrigidas; f) recomendações de mitigação e remediação; g) tempos de atendimento e tratamento; h) indicadores operacionais e executivos do serviço;

4.3.5. Emissão de relatório mensal consolidado com o mapa de redução de superfície de ataque, o percentual de exposições remediadas versus identificadas e a evolução do Índice de Exposição Residual do BDMG;

4.3.6. Apoio consultivo à definição e atualização contínua de planos de ação para remediação de vulnerabilidades e fortalecimento da postura de segurança cibernética do BDMG.

4.3.7. Fornecimento de orientações, boletins e relatórios contendo as principais remediações recomendadas para vulnerabilidades críticas, vulnerabilidades amplamente exploradas e ameaças com exploração ativa conhecida.

4.3.8. Compete à CONTRATADA executar as atividades de análise, classificação e priorização dos riscos associados às vulnerabilidades identificadas, bem como elaborar recomendações para seu tratamento, implementar medidas de mitigação lógica, acompanhar a execução das ações corretivas e realizar o reporte gerencial e operacional dos resultados e indicadores relacionados.

4.3.9. A execução de correções, ajustes de configuração, atualizações de software, aplicação de patches e demais atividades de remediação nos ativos do ambiente permanecerá sob responsabilidade das equipes do BDMG, observados os seus processos internos de gerenciamento de mudanças. Compete à CONTRATADA identificar, priorizar, correlacionar a vulnerabilidade ao respectivo patch ou medida corretiva, disponibilizar o pacote de correção e as instruções de aplicação por meio da solução de que trata o item 5, configurar e manter os anéis de implantação, as janelas de manutenção, as regras de aprovação, as exceções e os procedimentos de reversão homologados pelo Banco, acompanhar a execução e validar a efetiva correção, na forma do subitem 4.8. Os requisitos funcionais da solução previstos no item 5, inclusive os de implantação automática e silenciosa de patches, constituem exigências de capacidade da ferramenta a ser fornecida, e não atribuição de execução à CONTRATADA.

4.4. **Descoberta, Inventário e Cobertura de Ativos**

4.4.1. A CONTRATADA deverá manter processo contínuo de descoberta, inventário e avaliação de ativos de TI do BDMG, utilizando agentes, varreduras autenticadas e não autenticadas, bem como avaliação externa de ativos expostos à Internet. A varredura autenticada deverá ser adotada como padrão para todos os ativos que a suportem, não sendo admitida a utilização exclusiva de varreduras não autenticadas para fins de cobertura ou conformidade.

4.4.2. A CONTRATADA deverá monitorar e tratar falhas de cobertura decorrentes de problemas de autenticação, indisponibilidade de agentes ou inacessibilidade dos ativos, registrando e acompanhando as pendências por meio da ferramenta de ITSM.

4.4.3. Deverá, ainda, identificar ativos não inventariados, realizar a conciliação periódica entre os ativos descobertos, o inventário da solução e o inventário de ativos do BDMG, reportando divergências encontradas.

4.4.4. Os ativos que não admitam a instalação de agentes ou a realização de varreduras autenticadas deverão ser formalmente justificados, possuir controles compensatórios documentados e estar sujeitos à aprovação e revisão periódica pelo BDMG. A exclusão de ativos do escopo de avaliação dependerá de autorização formal do BDMG.

4.5. **Priorização Baseada em Risco**

4.5.1. A CONTRATADA deverá adotar modelo de priorização de vulnerabilidades baseado em risco, considerando, no mínimo, a severidade técnica da vulnerabilidade, probabilidade de exploração, evidências de exploração ativa, criticidade do ativo afetado, nível de exposição, existência de controles compensatórios e impacto ao negócio.

4.5.2. A priorização e a definição dos prazos de tratamento não poderão ser baseadas exclusivamente na pontuação CVSS, devendo considerar o contexto operacional e o risco efetivo para o BDMG.

4.5.3. O modelo de priorização, incluindo critérios, pesos, classificações e justificativas, deverá ser documentado, passível de auditoria, aprovado pelo BDMG e revisado periodicamente. Para cada vulnerabilidade, a solução deverá apresentar de forma transparente os fatores utilizados na classificação de risco e permitir a exportação das informações para análise e validação.

4.5.4. O BDMG poderá, a qualquer tempo e mediante justificativa, revisar ou redefinir a classificação de risco de ativos e vulnerabilidades, prevalecendo sua decisão para fins de priorização e tratamento.

4.5.5. Toda vulnerabilidade de severidade crítica com exploração ativa (KEV/CISA ou EPSS ≥ 0,7) presente no parque do BDMG gerará, obrigatoriamente e sem custo adicional: a) hipótese formal de caça a ameaças, a ser executada no âmbito do serviço de Caça a Ameaças (Threat Hunting), destinada a verificar indícios de exploração pretérita ou em curso no ambiente; e b) avaliação da existência de caso de uso de detecção compatível no Microsoft Sentinel, com criação ou ajuste de regra analítica quando ausente ou insuficiente. Ambas as providências serão registradas em chamado e concluídas em até 48 (quarenta e oito) horas contadas da identificação.

4.6. **Hardening e Avaliação da Postura de Segurança**

4.6.1. A CONTRATADA deverá executar, no mínimo trimestralmente, avaliações da postura de configuração de segurança dos ativos abrangidos pelo serviço, verificando a aderência às linhas de base de hardening reconhecidas pelo mercado, tais como CIS Benchmarks, DISA STIGs ou referências equivalentes aprovadas pelo BDMG. As avaliações deverão identificar desvios de configuração (configuration drift), classificá-los de acordo com sua criticidade, indicar os ativos afetados, apresentar recomendações de correção e permitir a identificação de padrões recorrentes de não conformidade.

4.6.2. As descobertas decorrentes das avaliações de postura de segurança deverão ser integradas ao processo de monitoramento e correlação de eventos de segurança,

permitindo o enriquecimento contextual dos alertas, a associação entre desvios de configuração e incidentes correlatos e a atualização dinâmica da classificação de risco dos ativos afetados.

4.6.3. Os serviços de hardening terão caráter consultivo e deverão resultar na emissão de recomendações técnicas de correção e fortalecimento da segurança dos ativos avaliados. Caberá exclusivamente ao BDMG analisar, aprovar e autorizar as alterações propostas, observados seus processos internos de gerenciamento de mudanças.

4.7. **Relatórios e Métricas**

4.7.1. A CONTRATADA deverá disponibilizar ao BDMG, até o 5º (quinto) dia útil de cada mês, relatório mensal da Gestão de Vulnerabilidades, composto por relatório executivo e relatório operacional, sem prejuízo dos demais relatórios previstos neste Termo de Referência.

4.7.2. O relatório executivo deverá apresentar, no mínimo, a evolução da exposição ao risco do ambiente, os principais riscos identificados, os ativos críticos afetados, os indicadores de remediação, a situação das exceções e aceites de risco, o cumprimento dos níveis de serviço contratados e os planos de ação para tratamento de desvios e indicadores fora das metas estabelecidas.

4.7.3. O relatório operacional deverá apresentar o detalhamento das vulnerabilidades identificadas, incluindo, no mínimo, ativos afetados, classificação de criticidade, nível de exposição, indicadores de explorabilidade, status do tratamento, área responsável, prazo de remediação e vínculo com os respectivos chamados de acompanhamento.

4.7.4. Todos os relatórios deverão ser acompanhados dos respectivos dados brutos, em formatos abertos e exportáveis, permitindo ao BDMG realizar auditorias, validações independentes e reprodução integral dos indicadores e cálculos apresentados, sem custos adicionais e sem dependência da CONTRATADA.

4.7.5. A solução deverá disponibilizar, no mínimo, os seguintes indicadores de desempenho da Gestão de Vulnerabilidades: a) tempo médio de remediação de vulnerabilidades (MTTR-V); b) percentual de vulnerabilidades remediadas; c) taxa de recorrência de vulnerabilidades; d) envelhecimento das vulnerabilidades abertas; e) percentual de cobertura dos ativos monitorados; f) volume de vulnerabilidades abertas por criticidade e área responsável; g) quantitativo de exceções e aceites de risco vigentes; e h) quantitativo de ativos descobertos e não inventariados.

4.7.6. Os indicadores e métricas deverão estar disponíveis em painel gerencial com atualização periódica, recursos de detalhamento (drill-down) até o nível de ativo e chamado, e mecanismos de filtragem, consulta e exportação para fins de gestão, auditoria e tomada de decisão.

4.8. **Prazos de Remediação e Validação**

Severidade	Reporte e abertura de chamado pela CONTRATADA	Prazo-alvo de remediação	Validação (reteste) pela CONTRATADA
Crítica com exploração ativa conhecida (KEV/CISA ou EPSS ≥ 0,7)	4 (quatro) horas	48 (quarenta e oito) horas	1 (um) dia útil
Crítica	24 (vinte e quatro) horas	7 (sete) dias corridos	2 (dois) dias úteis
Alta	48 (quarenta e oito) horas	15 (quinze) dias corridos	5 (cinco) dias úteis
Média	Relatório mensal	30 (trinta) dias corridos	5 (cinco) dias úteis
Baixa	Relatório mensal	90 (noventa) dias corridos	10 (dez) dias úteis

a) Os prazos da tabela acima contam-se da confirmação da vulnerabilidade pela CONTRATADA, após a análise e o tratamento de falso positivo de que trata o subitem 4.3.3, e aplicam-se de forma homogênea, independentemente do dia ou do horário da identificação.

b) São de responsabilidade da CONTRATADA, e sujeitos a apuração de níveis de serviço e a glosas, os prazos de reporte e abertura de chamado, a correlação da vulnerabilidade ao respectivo patch ou medida corretiva, a disponibilização do pacote de correção e das instruções de aplicação, o encaminhamento formal à área responsável do BDMG e a validação (reteste) da correção aplicada, contada esta da comunicação, pelo Banco, da conclusão da aplicação.

c) O prazo-alvo de remediação é meta institucional do BDMG, cuja execução compete às suas equipes, na forma do subitem 4.3.9, e o seu descumprimento não enseja glosa à CONTRATADA, ressalvada a hipótese de o atraso decorrer de ação, omissão ou atraso imputável à CONTRATADA nas obrigações da alínea anterior, hipótese em que o período correspondente lhe será atribuído.

d) A prorrogação de prazo-alvo de remediação e a não remediação dependerão de exceção ou de aceite de risco formal, com aprovador nominal, justificativa, controles compensatórios, prazo de validade e reavaliação obrigatória no vencimento, registrados na ferramenta de ITSM e refletidos nos relatórios e indicadores dos subitens 4.7.2 e 4.7.3.

e) Os prazos desta tabela não se confundem com os prazos de tratamento de incidentes de segurança do item 12, aplicáveis aos indicadores MTTA, MTTD, MTTC e MTTR, nem com as providências de caça a ameaças e de engenharia de detecção do subitem 4.5.5.

5. LICENÇAS DE USO DE SOLUÇÃO DE GESTÃO DE VULNERABILIDADES COM GERENCIAMENTO DE PATCHES

5.1. Como parte do escopo desta contratação, a CONTRATADA fornecerá o licenciamento e implantação de solução de software para gestão de vulnerabilidades, com capacidade de gerenciamento de patches (Patch Management).

5.2. As licenças de uso da solução de Gestão de Vulnerabilidades permanecerão sob titularidade direta do BDMG durante toda a vigência contratual e, em caso de extinção antecipada do contrato, até o término do período de licenciamento já pago, observado o modelo de licenciamento adotado pelo fabricante. O período de 12 (doze) meses de licenciamento indicado no quadro de itens será contado da emissão do Termo de Recebimento Definitivo (TRD), competindo à CONTRATADA assegurar, sem custo adicional e sem redução do período contratado, a plena disponibilidade das licenças, dos componentes e do suporte do fabricante durante a etapa de implantação, cujos custos se consideram diluídos na forma do subitem 7.1.1 da CLÁUSULA 7 – PAGAMENTO do contrato.

Descrição	Unidade de fornecimento	Quantitativo
Licenças de uso de solução de Gestão de Vulnerabilidades com Gerenciamento de Patches, por 12 (doze) meses	Ativos monitorados	1.200 (mil e duzentos)

5.3. O licenciamento da solução contemplará, para a totalidade dos ativos contratados, os módulos de Gestão de Vulnerabilidades, Patch Management e Policy Compliance, incluindo todas as funcionalidades nativas disponibilizadas pelo fabricante, sem restrições de uso ou cobrança adicional em função da quantidade de varreduras, avaliações de conformidade, correções aplicadas, agentes instalados ou integrações necessárias à operação da solução.

5.4. Todos os componentes necessários ao funcionamento da solução, incluindo sensores, scanners virtuais, agentes, conectores, APIs e mecanismos de integração nativos disponibilizados pelo fabricante, deverão estar contemplados no licenciamento ofertado, sem custos adicionais.

Arquitetura da Solução

5.5. A solução será fornecida e licenciada na modalidade Software as a Service (SaaS), incluindo as funcionalidades de Gestão de Vulnerabilidades, Gerenciamento de Patches e Policy Compliance. Serão admitidos apenas componentes on-premises estritamente necessários à descoberta de ativos, execução de varreduras autenticadas, coleta de dados e distribuição de patches, sem descaracterizar a arquitetura SaaS da solução.

5.6. A solução disponibilizará, de forma unificada ou por integração nativa fornecida e suportada pelo próprio fabricante, funcionalidades de descoberta de ativos, gerenciamento de vulnerabilidades, priorização baseada em risco e gerenciamento de patches, permitindo a correlação automática entre vulnerabilidades identificadas e respectivas ações de remediação.

Descoberta e Inventário

5.7. Manter inventário contínuo e automatizado de ativos de tecnologia, contemplando ambientes on-premises, nuvem pública, ambientes híbridos, dispositivos de usuário final, servidores, aplicações e serviços.

5.8. Realizar descoberta automática de ativos mediante agentes, scanners de rede, conectores de nuvem ou mecanismos equivalentes.

5.9. Identificar, no mínimo:

- Sistemas Windows;
- Sistemas Linux;
- Ativos em Microsoft Azure;
- Equipamentos de rede;
- Aplicações web;
- Máquinas virtuais;
- Bancos de dados;
- Serviços expostos à Internet;
- Aplicativos comerciais de uso corporativo.

5.10. Identificar ativos desconhecidos, não gerenciados ou não inventariados.

5.11. Agendar scans personalizados por periodicidade.

5.12. Escanear descoberta de rede por IP, CIDR e range.

5.13. Permitir tags estáticas e dinâmicas para ativos on-premises, nuvem, identidades e aplicações web.

5.14. Permitir atribuir criticidade por ativo.

Análise de Vulnerabilidades

5.15. Executar análises autenticadas e não autenticadas.

5.16. Identificar vulnerabilidades catalogadas por CVE.

5.17. Correlacionar vulnerabilidades com indicadores de exploração ativa, inteligência de ameaças e informações de exposição ao risco.

5.18. Permitir avaliação contínua de vulnerabilidades por meio de agentes instalados nos ativos monitorados.

5.19. Suportar avaliações sob demanda e agendadas.

5.20. Disponibilizar, de forma nativa e sem necessidade de desenvolvimento ou customização pelo BDMG, categorias, filtros, indicadores de ameaça, consultas ou painéis pré-definidos, mantidos e atualizados pelo fabricante, que permitam identificar, filtrar e priorizar, no mínimo, os seguintes conjuntos de vulnerabilidades:

a) Ameaças emergentes: vulnerabilidades sob monitoramento ativo da equipe de pesquisa do fabricante por potencial de exploração iminente, inclusive quando ainda não houver código de exploração público ou correção disponível;

b) Catálogo KEV da CISA: vulnerabilidades constantes do catálogo “Known Exploited Vulnerabilities” da CISA, com atualização automática a partir do catálogo oficial;

c) Maior prioridade de risco: vulnerabilidades presentes no ambiente classificadas segundo mecanismo de priorização de risco disponibilizado pela solução, permitindo identificar, no mínimo, as 10 (dez) vulnerabilidades de maior prioridade;

d) Exploração persistente: vulnerabilidades com evidência de exploração continuada, por período prolongado, em ataques direcionados ou em campanhas de malware ou ransomware;

e) Associadas a ransomware: vulnerabilidades com evidência de uso por grupos ou campanhas de ransomware;

f) Exploração ativa recente: vulnerabilidades com evidência de exploração ativa recente, conforme a inteligência de ameaças do fabricante;

g) Repercussão ou tendência relevante: vulnerabilidades com repercussão relevante recente em imprensa, boletins de segurança ou outras fontes públicas, ou identificadas por indicador de tendência equivalente.

5.20.1. As denominações e os mecanismos de identificação dos conjuntos estabelecidos nas alíneas anteriores são referenciais, não sendo exigida correspondência com nomenclaturas, categorias ou funcionalidades específicas de determinado fabricante. Será admitido o atendimento por meio de categorias, indicadores de ameaça, filtros, consultas predefinidas, painéis, mecanismos de priorização ou outros recursos nativos funcionalmente equivalentes da solução, desde que permitam obter os resultados requeridos sem desenvolvimento de código, scripts ou integrações específicas pelo BDMG.

Análise dinâmica de vulnerabilidades para aplicações Web (DAST/WAS)

5.21. Permitir a identificação, análise e reporte de vulnerabilidades em aplicações Web e APIs, possibilitando seu cadastramento e gerenciamento como ativos avaliados. As vulnerabilidades identificadas pelo componente de análise dinâmica de aplicações Web deverão ser disponibilizadas de forma integrada ao processo de Gestão de Vulnerabilidades da solução, permitindo sua identificação, classificação, priorização, acompanhamento, tratamento e reporte juntamente com as vulnerabilidades provenientes dos demais mecanismos de avaliação que compõem a solução.

5.22. Permitir a execução de varreduras de aplicações a partir de endereço IP, nome de domínio, FQDN, URL ou mecanismo equivalente de identificação do ativo.

5.23. Identificar vulnerabilidades e configurações inseguras relacionadas às principais categorias de riscos de segurança de aplicações Web reconhecidas pelo mercado, incluindo aquelas previstas no OWASP Top 10 e, quando aplicável, requisitos de segurança relacionados ao PCI DS.

5.24. Permitir avaliações destinadas a apoiar a verificação de requisitos de segurança aplicáveis ao PCI DSS.

INFORMAÇÃO CONTROLADA

5.25. Disponibilizar perfis, modelos ou configurações predefinidas de varredura, contemplando diferentes níveis de abrangência e profundidade dos testes.

5.26. Permitir a análise dos diferentes elementos identificados durante a navegação e interação com a aplicação, incluindo, conforme aplicável, cabeçalhos, cookies, formulários, links, parâmetros, conteúdos estruturados e elementos processados no lado cliente.

5.27. Permitir crawler isolado, scripts customizados, exclusão de URLs por regex e exclusão por extensão de arquivo.

5.28. Definir limites de URLs, diretórios, DOM, tamanho de resposta, redirects, tempo máximo, conexões HTTP e requisições por segundo.

5.29. Detectar congestionamento e limitar timeout e número máximo de timeouts antes de abortar.

5.30. Permitir a execução de varreduras sob demanda e mediante agendamento, inclusive de forma recorrente, com periodicidade configurável (diária, semanal, mensal).

5.31. Permitir a geração de notificações referentes à execução e aos resultados das varreduras, por correio eletrônico.

5.32. Permitir selecionar, habilitar, desabilitar ou configurar, de forma granular, os testes de segurança a serem executados, por vulnerabilidade, categoria de vulnerabilidade, técnica de ataque ou mecanismo equivalente disponibilizado pela solução.

5.33. Suportar a avaliação de aplicações Web acessíveis por protocolos HTTP e HTTPS, possibilitando, quando necessário, a utilização de cabeçalhos HTTP personalizados.

5.34. Suportar a avaliação dinâmica de APIs e serviços Web, contemplando diferentes padrões e arquiteturas utilizados pelo mercado, incluindo, no mínimo, APIs REST e serviços SOAP.

5.35. Suportar a avaliação de aplicações que requeiram autenticação, contemplando diferentes métodos e fluxos de autenticação utilizados pelas aplicações avaliadas.

5.36. Permitir a automação de fluxos de autenticação, navegação e interação necessários à realização das avaliações de segurança em aplicações que possuam fluxos de acesso dinâmicos ou complexos.

5.37. Exibir tendências temporais dos resultados e agregações por OWASP Top 10.

5.38. Permitir consultar, organizar, filtrar e apresentar os resultados por vulnerabilidade ou aplicação.

5.39. Apresentar evidências técnicas suficientes para análise e validação das vulnerabilidades identificadas, incluindo, conforme a natureza da vulnerabilidade, informações relativas às requisições, respostas, parâmetros ou demais elementos relevantes para sua comprovação e reprodução.

5.40. Disponibilizar, para as vulnerabilidades identificadas, informações que apoiem sua análise e tratamento, incluindo descrição, severidade, evidências técnicas, referências e recomendações para correção ou mitigação.

5.41. Permitir identificar vulnerabilidades relacionadas às tecnologias, componentes, bibliotecas, frameworks, servidores Web, servidores de aplicação e demais elementos identificáveis que componham as aplicações avaliadas, quando passíveis de detecção pela solução.

Priorização de Risco

5.42. Utilizar mecanismo de priorização baseada em risco que considere, no mínimo:

- Severidade CVSS;
- Exploração ativa;
- Existência de exploits públicos;
- Exposição do ativo;
- Criticidade do ativo para o negócio do BDMG;
- Contexto operacional do ambiente.

5.43. Disponibilizar recursos de correlação e de visualização gráfica das relações de exposição entre ativos, identidades, contas privilegiadas, softwares, aplicações web e recursos de nuvem, permitindo identificar, priorizar e investigar trajetórias de exploração plausíveis, classificá-las por criticidade e relacioná-las às táticas e técnicas do framework MITRE ATT&CK. Admite-se a entrega por meio de componentes integrados da mesma plataforma do fabricante, bem como a apresentação do mapeamento MITRE ATT&CK em matriz de táticas e técnicas, desde que correlacionada aos ativos, às identidades e às vulnerabilidades efetivamente identificados no ambiente do BDMG.

5.44. Fornecer visualização gráfica das relações de exposição e dos vetores de exploração identificados, com as conexões entre os objetos envolvidos, bem como apresentar evidências, origem e destino, técnicas MITRE ATT&CK associadas, indicadores de comprometimento, possíveis malwares relacionados, ações de mitigação recomendadas e histórico de eventos correlacionados, na medida em que tais informações estejam disponíveis na respectiva fonte de dados e observada a forma de entrega admitida no subitem 5.43.

5.45. Disponibilizar consultas e análises pré-configuradas para ambientes de rede, endpoints, Active Directory, permissões, credenciais, ransomware e vetores de ataque, permitindo a identificação de hosts, usuários e endereços IP suspeitos, observada a forma de entrega admitida no subitem 5.43.

5.46. Possuir dashboards executivos e operacionais contendo, no mínimo, ativos críticos vulneráveis, caminhos de ataque identificados, descobertas abertas, gravidade dos riscos, tendências de exposição e indicadores de evolução do ambiente, bem como permitir exportação das informações, arquivamento de descobertas, manutenção de trilha de auditoria e acompanhamento do tratamento por meio de status configuráveis.

Módulo Policy Compliance

5.47. A solução deverá possuir módulo integrado de avaliação de conformidade de configurações de segurança (Policy Compliance), permitindo verificar continuamente a aderência dos ativos às políticas de segurança definidas pelo BDMG.

INFORMAÇÃO CONTROLADA

5.48. O módulo de Policy Compliance deverá compartilhar o mesmo inventário de ativos e a mesma plataforma de gerenciamento da solução de gestão de vulnerabilidades, permitindo correlação entre descobertas de conformidade e vulnerabilidades identificadas.

Módulo Patch Management

5.49. O módulo de Patch Management deverá ser nativamente integrado à solução de gestão de vulnerabilidades, permitindo a associação automática entre vulnerabilidades identificadas e patches disponíveis para correção.

5.50. Permitir aprovação, rejeição, implantação e acompanhamento de patches a partir da console de gerenciamento de vulnerabilidades ou de console própria do módulo de Patch Management nativamente integrada a ela pelo fabricante, com autenticação federada única, inventário compartilhado e correlação automática entre a vulnerabilidade identificada e o patch aplicado.

5.51. Correlacionar vulnerabilidades identificadas com patches disponíveis.

5.52. Associar CVEs aos respectivos patches.

5.53. Identificar vulnerabilidades mitigadas após aplicação da correção.

5.54. Recalcular automaticamente o risco residual após a remediação.

5.55. Permitir a criação de grupos de implantação, janelas de manutenção e políticas de atualização.

5.56. Suportar estratégias de implantação piloto e implantação faseada.

5.57. Permitir aprovação automática por critérios definidos.

5.58. Possibilitar monitoramento do sucesso ou falha das implantações executadas.

5.59. Registrar aprovações, rejeições de patches e trilha completa de auditoria

5.60. Suportar o gerenciamento, distribuição, instalação, monitoramento e validação de correções (patches) para sistemas operacionais e aplicações de terceiros amplamente utilizadas em ambientes corporativos. O catálogo de sistemas operacionais e aplicações suportadas deverá contemplar, no mínimo, as seguintes categorias:

- Microsoft Windows 10 e posteriores;
- Microsoft Windows Server 2012 e posteriores;
- Linux, especialmente Ubuntu 22 e posteriores;
- Navegadores de internet;
- Suítes de produtividade e escritório;
- Ferramentas de colaboração, comunicação e videoconferência;
- Leitores, editores e manipuladores de documentos e arquivos PDF;
- Ambientes de execução (runtimes), frameworks e bibliotecas de software;
- Ferramentas de desenvolvimento, compilação, testes e integração contínua;

- Clientes de correio eletrônico;
- Clientes VPN e ferramentas de acesso remoto;
- Ferramentas de administração, gerenciamento e suporte remoto;
- Ferramentas de compactação e manipulação de arquivos;
- Soluções de virtualização e gerenciamento de máquinas virtuais;
- Bancos de dados, ferramentas de administração e clientes de acesso a bancos de dados;
- Servidores web, servidores de aplicação e componentes de middleware;
- Ferramentas de transferência de arquivos e protocolos seguros;
- Agentes e ferramentas de segurança da informação, incluindo antivírus, EDR, XDR, DLP, criptografia e controle de acesso;
- Demais aplicações corporativas suportadas pelo fabricante da solução.

5.61. A solução deverá permitir automatizar o fluxo de identificação, priorização e remediação das vulnerabilidades por meio da implantação de patches.

5.62. Permitir a execução de implantações automáticas e silenciosas de patches em estações de trabalho e servidores, mesmo na ausência de usuário autenticado ou sessão ativa, preservando a capacidade de monitoramento da execução, registro de logs, coleta de evidências, reporte de status e validação pós-instalação por meio do console central de gerenciamento.

5.63. Suportar workflows automatizados de correção baseados em regras de risco, criticidade ou SLA.

5.64. Permitir acompanhamento do ciclo completo de remediação, desde a identificação da vulnerabilidade até a validação da correção aplicada.

Integrações

5.65. Suportar integração com SIEM e mecanismos de automação e orquestração de segurança (SOAR).

5.66. Possuir APIs documentadas para integração com o Microsoft Sentinel.

5.67. Permitir o envio de informações de vulnerabilidades, risco e remediação para plataformas SIEM.

5.68. Permitir integração via API com plataformas ITSM corporativas de mercado.

5.69. Permitir abertura, atualização e encerramento automatizados de chamados associados a vulnerabilidades e processos de correção.

Relatórios e Indicadores

5.70. Disponibilizar relatórios e dashboards executivos e técnicos.

5.71. Permitir exportação de informações em, no mínimo, um dos seguintes formatos: HTML, CSV, XLSX ou PDF.

INFORMAÇÃO CONTROLADA

5.72. A solução deverá apresentar, no mínimo:

- Vulnerabilidades por criticidade;
- Tendência de redução de risco;
- Tempo médio de remediação de vulnerabilidades (MTTR-V);
- Ativos mais expostos;
- Patches pendentes;
- Conformidade de atualização;
- Evolução histórica de remediações.

5.73. Permitir criação de relatórios personalizados.

Console de Gerenciamento

5.74. Apresentar descrição, passos de correção e evidências/outputs para cada vulnerabilidade.

5.75. Fornecer RBAC, grupos de usuários, limitação de funções de varreduras e acesso a dashboards/relatórios.

5.76. Criptografar resultados e informações em repouso e trânsito.

5.77. Suportar métodos de autenticação por base local e SAML para uso de SSO (Single Sign-On) integrado ao Entra ID com suporte a MFA.

5.78. Orquestrar scanners ilimitados sem limite de quantidade na infraestrutura.

5.79. Alertar por e-mail sobre disponibilidade de resultados.

5.80. Configurar grupos dinâmicos por SO, IP, DNS, MAC, software instalado, Azure VM ID, Azure Resource ID e demais ativos avaliados.

5.81. Os resultados das varreduras realizadas no ambiente do BDMG, o histórico de vulnerabilidades, o registro das exceções e dos aceites de risco e o inventário de ativos serão retidos na solução por, no mínimo, 12 (doze) meses e exportáveis a qualquer tempo pelo BDMG em CSV, JSON e PDF, sem custo adicional.

5.82. As denominações de categorias, módulos, métricas e recursos empregadas neste item são referenciais e não vinculam a solução ofertada à nomenclatura de fabricante determinado. Será aceita solução que demonstre, por documentação oficial do fabricante, capacidade funcionalmente equivalente, ainda que sob outra denominação, outra métrica proprietária de priorização de risco ou outra organização de módulos, competindo ao BDMG avaliar a equivalência na análise da documentação exigida no subitem 2.5.8 do Anexo II – Condições e Documentos de Habilitação, facultada a realização de diligência junto à licitante, inclusive mediante apresentação de evidências, documentação complementar ou demonstração técnica, sem que isso configure Prova de Conceito nem implique alteração da proposta apresentada. A licitante indicará, em sua proposta, a correspondência entre cada requisito deste item e o recurso da solução ofertada que o atende, em aba própria da planilha da proposta.

6. ESCOPO E VOLUMETRIA DO AMBIENTE

6.1. Os quantitativos apresentados neste item refletem o ambiente de TI do BDMG na data de publicação do Edital e constituem exclusivamente a volumetria de referência para o dimensionamento das propostas técnica e comercial pelas licitantes. Tais quantitativos não representam, para a CONTRATADA, obrigação de disponibilização ou dimensionamento de capacidade da plataforma de SIEM, uma vez que o licenciamento da solução, bem como os custos associados à ingestão, retenção de dados, processamento e automação, é de responsabilidade exclusiva do BDMG.

6.2. Durante a vigência contratual, o ambiente tecnológico do BDMG poderá sofrer alterações em sua composição, volume ou arquitetura. Caso tais alterações impliquem, de forma comprovada, impacto relevante no escopo, esforço ou dimensionamento dos serviços contratados, as partes poderão promover os ajustes contratuais cabíveis, observada a legislação aplicável e as condições estabelecidas no contrato.

Escopo técnico	Descrição
Identidades (IdP)	800 (oitocentas) contas no Active Directory on-premises, sendo 764 (setecentos e sessenta e quatro) sincronizadas no Entra ID
Domain Controllers	2 (dois) DCs on-premises e 5 (cinco) DCs no Azure 2 (dois) DCs na DMZ
Servidores	76 (setenta e seis) servidores Windows e 48 (quarenta e oito) servidores Linux
Estações de trabalho	202 (duzentos e dois) desktops virtuais Windows 10/11 gerenciados pelo Active Directory 620 (seiscentos e vinte) endpoints físicos Windows 10/11 gerenciados pelo Intune
Nuvem	1 (uma) subscription Azure 3 (três) clusters AKS
Rede	100 ativos de rede (switches e roteadores) VPN site-to-site entre BDMG e o Azure
Ferramentas de segurança	4 (quatro) firewalls Check Point com IDS/IPS integrado WAF Akamai 15 (quinze) proxies NGINX/Apache SentinelOne EDR/XDR Microsoft Defender for Office 365 Cofre de senhas (PAM)
Volumetria de ingestão de logs do SIEM	o consumo médio atual do SIEM é de 62 GB/dia (sessenta e dois gigabytes por dia), correspondentes a aproximadamente 800 EPS (oitocentos eventos por segundo). Para fins de dimensionamento

INFORMAÇÃO CONTROLADA

Escopo técnico	Descrição
	desta contratação, o BDMG projeta crescimento de aproximadamente 100% (cem por cento) sobre essa linha de base, resultando em referência de até **124 GB/dia** (cento e vinte e quatro gigabytes por dia) e **1.600 EPS** (mil e seiscentos eventos por segundo

6.3. Durante a vigência contratual, o BDMG ingressará no Sistema de Pagamentos Brasileiro (SPB), com conta no Sistema de Transferência de Reservas (STR) e acesso por meio da Rede do Sistema Financeiro Nacional (RSFN). Os ativos, as identidades, os acessos privilegiados, as conexões e as fontes de log que suportarem essa participação integrarão o ambiente monitorado pelos serviços contratados, observado o disposto no subitem 6.2, competindo à CONTRATADA integrar as respectivas fontes, desenvolver os casos de uso, as regras analíticas e os playbooks de resposta aplicáveis e refletir esse escopo nos relatórios e indicadores de que tratam os itens 9 e 11.13.

6.4. O escopo de análise dinâmica de aplicações web (DAST/WAS) de que tratam os subitens 5.21 a 5.41 compreende 10 (dez) aplicações web, identificadas por nome de domínio totalmente qualificado (FQDN), cuja relação nominal será fornecida pelo BDMG à CONTRATADA na reunião inicial de alinhamento de que trata o subitem 11.2. O licenciamento, os componentes e os quantitativos necessários à análise dessas aplicações integram o item 3 do quadro de itens do subitem 1.1 e deverão estar integralmente contemplados na proposta, sem custo adicional. A substituição de aplicações web dentro do mesmo quantitativo não ensejará acréscimo de preço.

7. PERFIS E QUALIFICAÇÃO TÉCNICA DA EQUIPE DA CONTRATADA

7.1. A CONTRATADA será responsável pelo dimensionamento, disponibilização, gestão e supervisão da equipe técnica necessária à execução dos serviços, garantindo profissionais qualificados e em quantidade suficiente para o atendimento dos níveis de serviço e demais obrigações contratuais.

7.2. Eventuais substituições de profissionais deverão ocorrer por profissionais com qualificação e experiência equivalentes ou superiores, sem impacto à continuidade ou à qualidade dos serviços.

7.3. A CONTRATADA assegurará a adequada segregação de funções, a capacidade operacional e a disponibilidade dos recursos humanos necessários à prestação dos serviços.

7.4. Caberá exclusivamente à CONTRATADA o cumprimento de todas as obrigações trabalhistas, previdenciárias, tributárias, fiscais e demais encargos decorrentes da contratação de seus profissionais, não se estabelecendo qualquer vínculo empregatício ou relação de subordinação entre estes e o BDMG, observada a legislação aplicável e as disposições deste Termo de Referência e de seus anexos.

INFORMAÇÃO CONTROLADA

7.5. A CONTRATADA comunicará previamente ao BDMG, com antecedência mínima de 10 (dez) dias úteis, a substituição de qualquer profissional designado nominalmente para a execução deste contrato, apresentando o substituto com qualificação, experiência e certificações iguais ou superiores às do substituído e a respectiva comprovação de vínculo trabalhista.

7.6. O BDMG poderá solicitar, mediante justificativa formal, o descredenciamento de profissional da CONTRATADA nas hipóteses de: a) violação das obrigações de sigilo ou da Política de Segurança da Informação e Cibernética do BDMG; b) uso indevido de credenciais ou acesso a dados além do estritamente necessário à execução dos serviços; ou c) conduta incompatível com o Código de Ética do BDMG. A substituição ocorrerá em até 5 (cinco) dias úteis, sem ônus para o Banco.

7.7. Na hipótese de descredenciamento determinado pelo BDMG na forma do subitem anterior, a CONTRATADA revogará todos os acessos do profissional aos ambientes, consoles, repositórios e portais relacionados a este contrato em até 24 (vinte e quatro) horas contadas da solicitação, comunicando o fato ao Fiscal do Contrato e apresentando evidência formal da revogação. Nas demais hipóteses de desligamento, afastamento ou remanejamento do profissional, aplica-se o prazo de 5 (cinco) dias úteis.

7.8. Os quantitativos definidos nesta seção representam requisitos mínimos de capacidade operacional, não constituindo limite máximo para a composição da equipe. A CONTRATADA poderá adotar modelo de alocação compartilhada de recursos, escalas de revezamento, plantões e regime de sobreaviso, desde que sejam integralmente atendidos os requisitos de disponibilidade, qualidade, tempestividade e continuidade dos serviços contratados. Os quantitativos mínimos da tabela do subitem 7.9 correspondem à capacidade simultaneamente disponível em cada turno, e não ao total de profissionais alocados: a CONTRATADA assegurará, em todos os turnos e em todos os dias do ano, a disponibilidade de, no mínimo, 1 (um) Analista de SOC Nível 1 e 1 (um) Analista de SOC Nível 2 em atendimento efetivo, e de Analista de SOC Nível 3 em atendimento ou em sobreaviso acionável nos prazos de escalonamento do subitem 12.14, dimensionando o respectivo contingente de forma a cobrir escalas, férias, afastamentos e absenteísmo.

7.9. A tabela a seguir estabelece os quantitativos mínimos de profissionais exigidos em cada perfil para a execução dos serviços.

Perfil	Qtd. mínima obrigatória	Regime de trabalho
Gestor do SOC (Gerente/Coordenador/Supervisor)	1	Remoto
Analista de SOC Nível 1 (N1)	1	Remoto
Analista de SOC Nível 2 (N2)	1	Remoto
Analista de SOC Nível 3 (N3)	1	Remoto
Analista de Gestão de Vulnerabilidades	1	Remoto
Analista de Segurança Sênior Nível 3 (N3) Dedicado	1	Híbrido
Technical Account Manager (TAM)	1	Remoto

Perfil	Qtd. mínima obrigatória	Regime de trabalho
Analista de Inteligência de Ameaças (Threat Intelligence)	1	Remoto

7.10. A CONTRATADA deverá disponibilizar profissional para atuar como **Gestor do SOC**, com nível sênior, formação superior na área de Tecnologia da Informação ou equivalente e experiência mínima comprovada de 5 (cinco) anos em gestão de operações de segurança cibernética, centros de operações de segurança ou sistemas de gestão da segurança da informação.

a) O profissional deverá possuir certificação Certified Information Systems Security Professional (CISSP) e, adicionalmente, pelo menos uma das seguintes certificações ou equivalentes reconhecidas pelo mercado: Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), GIAC Security Essentials (GSEC), GIAC Certified Incident Handler (GCIH), CompTIA Cybersecurity Analyst (CySA+).

7.11. Os **Analistas de SOC Nível 1** deverão possuir formação na área de Tecnologia da Informação ou equivalente e, no mínimo, uma das seguintes certificações:

a) CompTIA Security+;
b) Microsoft Security Operations Analyst (SC-200);
c) Blue Team Level 1 (BTL1);
d) GIAC Security Essentials (GSEC);
e) certificação equivalente reconhecida pelo mercado.

7.12. Os **Analistas de SOC Nível 2** deverão possuir formação na área de Tecnologia da Informação ou equivalente e, no mínimo, uma das seguintes certificações:

a) GIAC Certified Incident Handler (GCIH);
b) CompTIA CySA+;
c) Microsoft Security Operations Analyst (SC-200);
d) GIAC Security Essentials (GSEC);
e) Blue Team Level 1 (BTL1);
f) certificação equivalente reconhecida pelo mercado.

7.13. Os **Analistas de SOC Nível 3** deverão possuir formação na área de Tecnologia da Informação ou equivalente, experiência comprovada em operações de segurança cibernética e, no mínimo, uma das seguintes certificações:

a) GIAC Certified Incident Handler (GCIH);
b) GIAC Security Essentials (GSEC);
c) GIAC Certified Intrusion Analyst (GCIA);
d) CompTIA CySA+;

INFORMAÇÃO CONTROLADA

e) Microsoft Security Operations Analyst (SC-200);
f) Certified Ethical Hacker (CEH);
g) certificação equivalente reconhecida pelo mercado.

7.14. Os **Analistas de Gestão de Vulnerabilidades** deverão atender aos requisitos mínimos de qualificação técnica previstos para o perfil de Analista de SOC Nível 3, possuindo obrigatoriamente certificação do fabricante na solução de Gestão de Vulnerabilidades fornecida pela CONTRATADA.

7.15. A CONTRATADA deverá manter, durante toda a vigência do contrato, 1 (um) **Analista de Segurança Sênior Nível 3** dedicado à execução dos serviços contratados e formalmente designado como ponto focal técnico junto ao BDMG.

7.15.1. O profissional deverá atender aos requisitos mínimos de qualificação técnica previstos para o perfil de Analista de SOC Nível 3, possuindo obrigatoriamente a certificação Microsoft Security Operations Analyst (SC-200), válida e vigente.

7.15.2. Este profissional atuará prioritariamente nos serviços de Engenharia de Detecção e Otimização do SIEM e Caça a Ameaças (Threat Hunting), incluindo a implementação, manutenção e otimização dos casos de uso, regras analíticas, automações e demais mecanismos de monitoramento e detecção no Microsoft Sentinel.

7.15.3. Além das atividades mencionadas, compete ao Analista de Segurança Sênior Nível 3 executar e apoiar atividades táticas e operacionais relacionadas aos serviços contratados, incluindo investigação de ameaças, resposta a incidentes, gestão de vulnerabilidades, proposição de melhorias, elaboração de recomendações técnicas e apoio à evolução contínua dos controles de segurança cibernética do BDMG.

7.15.4. O profissional atuará em regime de trabalho híbrido, com presença obrigatória nas dependências do BDMG, em Belo Horizonte/MG, por no mínimo 3 (três) dias úteis por semana, no horário de funcionamento do Banco, e conforme cronograma previamente alinhado com a Superintendência de Tecnologia do BDMG, realizando remotamente suas atividades nos demais dias da jornada semanal.

7.15.5. O profissional permanecerá vinculado à prestação dos serviços durante toda a vigência contratual, sendo vedada a sua substituição sem prévia anuência do BDMG, exceto em situações excepcionais devidamente justificadas pela CONTRATADA e formalmente aprovadas pelo BDMG. Em qualquer hipótese de substituição, férias, ausência, afastamento ou desligamento, a CONTRATADA designará formalmente substituto apto e previamente treinado, de perfil e certificação equivalentes aos exigidos neste Termo de Referência, assegurando cobertura integral do posto, com comunicação imediata ao BDMG e reposição definitiva em até 15 (quinze) dias corridos.

7.15.6. O posto não preenchido por prazo superior ao previsto sujeitará a CONTRATADA a glosa proporcional aos dias de ausência, calculada sobre o valor mensal dos serviços.

7.15.7. As despesas de deslocamento, transporte, hospedagem e alimentação decorrentes do trabalho presencial, correm por conta da CONTRATADA e deverão estar integralmente

INFORMAÇÃO CONTROLADA

incluídas no preço proposto, sendo vedada qualquer cobrança adicional a esse título, a qualquer tempo e sob qualquer denominação.

7.15.8. Excepcionalmente, quando o BDMG determinar a instalação presencial de Sala de Guerra, o profissional deverá comparecer às dependências do Banco em até 2 (duas) horas contadas da convocação, independentemente do dia ou horário, prevalecendo essa regra específica sobre as demais disposições deste item.

7.15.9. O BDMG disponibilizará, durante os períodos de trabalho presencial do Analista de Segurança Sênior Nível 3 Dedicado, posto de trabalho adequado em suas dependências, bem como os acessos físicos necessários ao desempenho das atividades.

7.15.10. A presença física do Analista de Segurança Sênior Nível 3 Dedicado nas instalações do BDMG não implicará qualquer flexibilização das regras de segurança estabelecidas, nem autorizará acesso local à infraestrutura tecnológica do Banco, compartilhamento de credenciais, utilização de contas genéricas ou conexão direta à rede corporativa sem observância dos mecanismos de controle previstos neste contrato.

7.16. Além dos perfis descritos, a CONTRATADA designará, sem custo adicional, um **Technical Account Manager (TAM)** como ponto focal técnico e de relacionamento com o BDMG durante toda a vigência contratual. O TAM será responsável por coordenar as atividades operacionais e táticas dos serviços, acompanhar indicadores de desempenho e níveis de serviço (SLA), apoiar a gestão de incidentes críticos, conduzir reuniões periódicas de acompanhamento, coordenar escalonamentos técnicos junto às equipes especializadas da CONTRATADA e atuar como interface principal entre o BDMG e a CONTRATADA para questões relacionadas à prestação dos serviços.

a) O TAM deverá possuir experiência compatível com o objeto contratado e estará disponível em horário comercial para atividades de governança, planejamento, acompanhamento de planos de ação e suporte à gestão contratual.

b) Em incidentes classificados como P1 ou P2, o TAM deverá ser imediatamente acionado pela CONTRATADA, acompanhando o tratamento da ocorrência até sua normalização, mantendo o BDMG informado sobre a evolução, riscos, impactos e ações de mitigação.

c) Os dados de contato do TAM e de seu substituto serão fornecidos ao BDMG durante a implantação dos serviços, devendo qualquer alteração ser comunicada formalmente com antecedência mínima de 15 (quinze) dias corridos.

d) A atuação do TAM não substitui as obrigações operacionais, os canais de atendimento, os níveis de escalonamento, nem afasta a responsabilidade da CONTRATADA pelo cumprimento dos SLAs e demais obrigações contratuais.

7.17. A CONTRATADA deverá disponibilizar profissional para atuar como Analista de Inteligência de Ameaças (Threat Intelligence), responsável pela execução das atividades do item 3.7, com formação na área de Tecnologia da Informação ou equivalente e experiência comprovada em análise de inteligência de ameaças cibernéticas.

a) O profissional deverá possuir, no mínimo, uma das seguintes certificações ou equivalente reconhecida pelo mercado: Certified Threat Intelligence Analyst (CTIA); GIAC Cyber Threat Intelligence (GCTI); Certified Cyber Threat Intelligence Analyst (CCTIA); ou Blue Team Level 2 (BTL2).

b) O profissional não poderá ser o mesmo designado para o cumprimento dos quantitativos mínimos dos perfis de Analista de SOC Nível 1, Nível 2 e Nível 3 e de Analista de Segurança Sênior Nível 3 Dedicado, admitida a atuação integrada e o compartilhamento de recursos entre clientes da CONTRATADA, na forma do subitem 7.8.

c) A atuação poderá ser remota, assegurada a participação nas reuniões de governança tática e estratégica de que trata o subitem 11.15 sempre que convocada pelo BDMG.

7.18. As certificações exigidas nesta seção deverão permanecer vigentes durante toda a execução contratual, admitido o prazo de até 3 (três) meses, contado da expiração, para a apresentação da renovação ou de certificação equivalente. Não renovada a certificação nesse prazo, o profissional será substituído na forma dos subitens 7.2 e 7.5.

8. FERRAMENTA DE ITSM E CANAIS DE ATENDIMENTO DA CONTRATADA

8.1. Na ocasião da implantação dos serviços gerenciados de SOC, a CONTRATADA deverá disponibilizar ao BDMG, durante toda a vigência contratual, uma ferramenta de Gerenciamento de Serviços (ITSM), acessível via internet, para utilização por, no mínimo, 10 (dez) usuários nomeados da equipe técnica do Banco.

8.2. A ferramenta de ITSM deverá constituir solução corporativa amplamente adotada no mercado, tais como ServiceNow, BMC Helix, Jira Service Management e ManageEngine ServiceDesk Plus, para registro, atualização e encerramento de chamados e incidentes de segurança, admitindo-se soluções equivalentes mediante aderência funcional aos requisitos especificados.

8.3. A ferramenta de ITSM deverá registrar e manter todas as evidências produzidas ou coletadas durante o tratamento de eventos, incidentes e requisições, garantindo sua rastreabilidade e integridade, bem como todas as informações necessárias à apuração dos níveis de serviço e à emissão dos relatórios gerenciais e de indicadores relacionados aos serviços contratados.

8.4. Cada evento de segurança gerado ou correlacionado no Microsoft Sentinel do BDMG deverá resultar, de forma automática, na abertura de um chamado na ferramenta de ITSM da CONTRATADA, devidamente classificado como evento de segurança e contendo as informações necessárias ao seu tratamento, rastreabilidade e auditoria.

8.5. A ferramenta de ITSM deverá suportar integração bidirecional, por meio de APIs, com o Microsoft Sentinel do BDMG, contemplando a abertura, atualização e encerramento automáticos de chamados, bem como o espelhamento de registros, anexos, históricos e carimbos de data e hora. A solução deverá atender integralmente aos requisitos de acesso, exportação de dados, trilha de auditoria, retenção e titularidade dos registros estabelecidos neste Termo de Referência.

INFORMAÇÃO CONTROLADA

8.6. A CONTRATADA disponibilizará, sem custo adicional e durante toda a vigência contratual, central de atendimento própria, operando em regime 24x7x365, para abertura, acompanhamento, escalonamento e encerramento de chamados e incidentes de segurança.

8.7. O atendimento será realizado, no mínimo, por meio de: a) portal ITSM acessível via internet, com autenticação multifator e acesso para até 10 usuários do BDMG; b) telefone 0800 com atendimento humano em português; c) WhatsApp corporativo institucional; d) correio eletrônico institucional com geração automática de chamado; e) sala de resposta a incidentes (war room), obrigatória para incidentes P1 e sob demanda do BDMG para demais prioridades.

8.8. Os contatos, procedimentos de acionamento e matriz de escalonamento serão informados na implantação dos serviços e qualquer alteração deverá ser comunicada ao BDMG com antecedência mínima de 15 (quinze) dias corridos, salvo situações de força maior.

8.9. Todos os canais permanecerão disponíveis 24x7x365 para registro de incidentes de segurança. Para demandas administrativas e chamados de baixa criticidade (P3 e P4), admite-se atendimento humano em horário comercial, mantendo-se o portal ITSM e o correio eletrônico disponíveis para registro a qualquer tempo.

8.10. Todo acionamento deverá gerar registro obrigatório na ferramenta ITSM, que constituirá o registro oficial para apuração de SLA, medição e auditoria.

8.11. Os chamados deverão conter, no mínimo, identificação única, data e hora de abertura, solicitante, descrição da ocorrência, classificação de prioridade, responsável pelo atendimento, ações executadas e data e hora de encerramento.

8.12. Os prazos de SLA serão contados a partir do primeiro contato realizado pelo BDMG em qualquer canal oficial. Quando o registro inicial ocorrer fora do ITSM, a CONTRATADA deverá formalizá-lo na ferramenta em até 15 (quinze) minutos, preservando o horário original do acionamento.

8.13. A CONTRATADA deverá confirmar a abertura do chamado ao solicitante, informando o número do protocolo dentro dos prazos estabelecidos para o MTTA.

8.14. Para incidentes críticos (P1 e P2), será assegurado atendimento humano por telefone ou WhatsApp, vedado o atendimento exclusivamente automatizado.

8.15. O WhatsApp corporativo destina-se exclusivamente ao acionamento, comunicação de status e coordenação do atendimento, sendo vedado o compartilhamento de informações sensíveis ou evidências técnicas por esse canal.

8.16. A CONTRATADA manterá matriz de escalonamento atualizada, contendo os contatos dos responsáveis pelos níveis N1, N2 e N3, do Gestor do SOC e do preposto.

8.17. A indisponibilidade de qualquer canal não suspenderá os SLAs contratuais, devendo a CONTRATADA assegurar a continuidade do atendimento pelos canais remanescentes.

8.18. Os registros de atendimento, incluindo gravações e histórico de comunicações, deverão ser mantidos por no mínimo 12 (doze) meses e disponibilizados ao BDMG mediante solicitação.

INFORMAÇÃO CONTROLADA

8.19. A CONTRATADA fornecerá as credenciais de acesso ao portal ITSM e treinamento para sua utilização, garantindo a consulta e exportação dos dados dos chamados pelo BDMG.

8.20. Não será admitida cobrança adicional pela disponibilização dos canais de atendimento, quantidade de usuários ou volume de chamados, estando tais custos incluídos no valor contratado.

9. PORTAL DE VISIBILIDADE EXECUTIVA E OPERACIONAL

9.1. A CONTRATADA disponibilizará ao BDMG, sem custo adicional e durante toda a vigência contratual, portal web de visualização por painéis (dashboards) para acompanhamento executivo e operacional e governança dos serviços contratados, integrado, de forma nativa ou por API, ao Microsoft Sentinel do BDMG, à ferramenta de ITSM do item 8, à solução de Gestão de Vulnerabilidades do item 5 e ao repositório Git do subitem 3.5.9, preferencialmente por meio de workbooks no Microsoft Sentinel do BDMG. Alternativamente, poderá ser utilizado portal da própria CONTRATADA, desde que assegurados os requisitos de acesso, exportação, rastreabilidade, segurança, retenção de histórico e reversibilidade previstos neste Termo de Referência.

9.2. O portal deverá consolidar, em ambiente único, informações relativas aos serviços contratados, contemplando, no mínimo:

- MTTA, MTTD, MTTC e MTTR por severidade, com as definições do subitem 1.4, e Tempo do Ciclo de Investigação, na forma do subitem 12.15;;
- Taxa de falsos positivos;
- Incidentes por criticidade;
- Percentual de automação aplicada;
- Saúde de conectores e fontes de dados;
- Volume de dados ingeridos e custos estimados;
- Cobertura de ativos e matriz MITRE ATT&CK;
- Vulnerabilidades abertas e aderência aos SLAs;
- Indicadores de exposição cibernética;
- Conformidade de patch management;
- Indicadores mensais de Níveis de Serviço;
- Indicadores de disponibilidade mensal dos serviços;
- Indicadores de SLA de chamados;
- Backlog de chamados;
- Indicadores de Threat Hunting;
- Indicadores de automação e eficiência operacional;

9.3. O acesso ao portal observará autenticação multifator (MFA), contas nominais, perfis de permissão, no mínimo executivo e operacional, e integração com o Microsoft Entra ID do BDMG por SAML 2.0. A CONTRATADA disponibilizará, no mínimo, 5 (cinco) usuários nominais, sem custo adicional.

INFORMAÇÃO CONTROLADA

9.4. Os dados do portal serão atualizados de forma automática, sem intervenção manual da CONTRATADA ou do BDMG, nos seguintes intervalos máximos:

a) 15 (quinze) minutos, para os indicadores operacionais e de SLA e para o painel de incidentes do subitem 9.14, em consonância com o subitem 12.21;

b) 24 (vinte e quatro) horas, para as informações de vulnerabilidades, cobertura de ativos, patch management e regras de detecção e para as análises do subitem 9.15.

9.5. Todos os indicadores deverão permitir rastreabilidade até os registros de origem, incluindo incidentes, chamados, ativos e vulnerabilidades, bem como disponibilizar memória de cálculo, fórmulas e critérios utilizados em sua apuração.

9.6. O BDMG poderá exportar dados e relatórios em formatos CSV, JSON, XLSX e PDF, além de acessar as informações por meio de API REST segura, sem necessidade de intervenção da CONTRATADA.

9.7. O Portal manterá histórico de informações por todo o período contratual, disponibilizando consulta imediata de, no mínimo, 12 (doze) meses de dados.

9.8. O Portal deverá apresentar disponibilidade mínima mensal de 99,5%, excetuadas janelas de manutenção previamente comunicadas pelo menos 5 (cinco) dias úteis antes de sua execução.

9.9. É vedada qualquer cobrança adicional relacionada a usuários, perfis, indicadores, painéis, relatórios, integrações, APIs, retenção de histórico ou volume de dados processados.

9.10. Ao término do contrato ou durante a transição assistida, a CONTRATADA entregará ao BDMG a base histórica completa dos indicadores e respectivos dados-fonte em formatos abertos (CSV e JSON), acompanhados da documentação técnica necessária para sua interpretação.

9.11. O portal deverá estar disponível, com os painéis deste item em funcionamento e dados reais do período, até a conclusão da fase de implantação, constituindo requisito para a emissão do Termo de Recebimento Definitivo (TRD), na forma da alínea 'c' do subitem 11.11.

9.12. Os dados do BDMG deverão permanecer segregados logicamente de outros clientes, trafegar exclusivamente por canais criptografados e ser utilizados somente para execução contratual, observadas a LGPD e as obrigações de confidencialidade previstas no contrato.

9.13. Os indicadores de tempo e de incidentes do subitem 9.2 poderão ser filtrados por período, severidade e status do incidente e exibirão a série histórica, a tendência e o percentual de cumprimento das metas dos subitens 12.14 e 12.15, apurados na forma dos subitens 12.6 e 12.7.

9.14. O portal exibirá os incidentes abertos no Microsoft Sentinel, bem como o histórico dos encerrados, informando, para cada incidente, no mínimo:

a) identificador, severidade e data e hora de detecção;

b) status atual do tratamento;

c) Analista de SOC designado e respectivo nível (N1, N2 ou N3), com a data e hora da última atuação registrada, destacando-se os incidentes sem analista designado;

INFORMAÇÃO CONTROLADA

d) link direto, gerado automaticamente e sem intervenção manual, para o chamado correspondente na ferramenta de ITSM, aberto na forma dos subitens 8.4 e 8.5.

9.15. O portal exibirá análises de risco e de tendência, incluindo a previsão de picos de alertas e de incidentes, geradas por agentes ou mecanismos de Inteligência Artificial integrados ao Microsoft Sentinel do BDMG e apresentadas nos próprios painéis como apoio à decisão operacional e executiva, com indicação do período de dados considerado e da data de geração de cada análise. Aplicam-se a esses mecanismos, generativos ou não, os subitens 3.8.2 a 3.8.7. Para os fins do subitem 3.8.5, fica autorizada a sua calibração com dados do BDMG exclusivamente para as análises do próprio Banco, constituindo os modelos resultantes propriedade do BDMG, entregues na forma do subitem 14.1, vedado seu uso em benefício de terceiros. O portal e esses mecanismos não poderão gerar consumo, no ambiente de nuvem do BDMG, de serviços distintos dos recursos nativos do Microsoft Sentinel referidos no subitem 1.8, salvo autorização prévia do Banco, precedida de estimativa de custo, observado, quanto ao volume ingerido, o subitem 3.5.26.

9.16. O portal exibirá mapa das regras de detecção, conectado ao repositório Git de que trata o subitem 3.5.9, contendo, no mínimo:

a) regras de detecção ativas, organizadas por conector ou fonte de dados;

b) conectores e fontes de dados ingeridos no Microsoft Sentinel sem regra de detecção associada;

c) distribuição das regras por táticas e técnicas do framework MITRE ATT&CK, com a cobertura e as lacunas de que trata o subitem 3.5.5;

d) divergências entre as regras versionadas no repositório e as regras efetivamente ativas no Microsoft Sentinel;

e) anomalias no comportamento das regras identificadas por agentes de Inteligência Artificial, como regras sem disparo em período parametrizável pelo BDMG ou com variação de disparos fora do padrão histórico.

9.17. O portal será integrado à solução de Gestão de Vulnerabilidades do item 5 e exibirá as visões de risco de vulnerabilidades do ambiente do BDMG, contendo, no mínimo:

a) ativos cobertos e não cobertos pela gestão de vulnerabilidades, conciliados com o inventário de ativos do BDMG, na forma do subitem 4.4.3;

b) ações de correção prioritárias, ordenadas pelo modelo de priorização baseada em risco do subitem 4.5, inclusive quanto à criticidade dos ativos;

c) MTTR-V por severidade (crítica, alta, média e baixa).

9.18. O portal exibirá também os indicadores dos subitens 3.4.8-A (HIIRR), 3.5.23-A (DEY), 3.9.7 (autonomia e eficiência) e 12.15-A (IFP por regra analítica), a linha de base do subitem 12.11-A e o executor de cada ação registrada, na forma do subitem 12.7-C.

10. LOCAL DE PRESTAÇÃO DOS SERVIÇOS

10.1. Os serviços objeto deste Termo de Referência serão executados predominantemente de forma remota, por meio de acesso seguro ao ambiente de TI do BDMG. As atividades presenciais do profissional designado para a função de Analista de Segurança Sênior Nível 3 Dedicado serão desempenhadas, conforme item 7.15.4, nas dependências do BDMG, situadas na Rua da Bahia, nº 1.600, Bairro Lourdes, Belo Horizonte/MG.

11. FORMA E CONDIÇÕES DE EXECUÇÃO DO OBJETO

11.1. A implantação dos serviços deverá ser formalizada por Plano de Implantação e Termo de Recebimento Definitivo (TRD), com prazo de até 60 (sessenta) dias corridos contados da assinatura do contrato. A implantação constitui escopo próprio do objeto, distinto do escopo de operação continuada, e não é objeto de remuneração específica, na forma do subitem 7.1.1 da CLÁUSULA 7 – PAGAMENTO do contrato.

Fase 1 – Planejamento e Projeto Executivo

11.2. Em até 10 (dez) dias corridos, contados da assinatura do contrato, a CONTRATADA realizará reunião inicial de alinhamento com o BDMG, destinada a esclarecer as obrigações contratuais e as condições de início da prestação dos serviços, com a presença obrigatória do preposto, do Gestor do SOC e do Gerente de Projetos da CONTRATADA.

11.3. Em até 10 (dez) dias corridos contados da realização da reunião inicial, a CONTRATADA deverá apresentar ao BDMG o Plano de Implantação, contendo, no mínimo:

a) descrição dos serviços a serem implantados, da estratégia de transição e do fluxo de monitoramento, detecção, escalonamento, tratamento e encerramento de incidentes de segurança;
b) arquitetura e topologia lógica das integrações previstas, contemplando as fontes de dados, conectores, fluxos de comunicação e respectivos métodos de coleta e ingestão;
c) requisitos, premissas, dependências e atividades de responsabilidade do BDMG, com indicação dos prazos necessários para sua execução;
d) cronograma detalhado de implantação, contemplando marcos, entregas, responsáveis e critérios de aceite;
e) plano de comunicação, matriz de escalonamento e matriz preliminar de responsabilidades (RACI);
f) plano de revisão, racionalização e validação do baseline de casos de uso e regras analíticas existentes;
g) relação nominal dos profissionais alocados em cada perfil contratual, acompanhada da documentação comprobatória de formação, certificações, experiência profissional e vínculo com a CONTRATADA.

11.4. O BDMG terá até 10 (dez) dias para examinar e aprovar ou rejeitar, de forma fundamentada, o Plano de Implantação; em caso de rejeição, a CONTRATADA sanará as pendências em até 5 (cinco) dias, sem ônus adicional para o Banco. A aprovação do Plano é condição para o início da fase de implantação e ativação.

Fase 2 – Implantação e Ativação

11.5. Após o aceite do Plano de Implantação pelo BDMG, a CONTRATADA iniciará as atividades de implantação e ativação de cada serviço contratado, de acordo com o Projeto Executivo.

11.6. Nessa fase, a CONTRATADA também fornecerá ao BDMG as instruções e credenciais de acesso à Ferramenta de ITSM e ao Portal de Visibilidade Executiva e Operacional para os profissionais indicados pelo Banco.

INFORMAÇÃO CONTROLADA

11.7. A prorrogação do prazo máximo de implantação e ativação dos serviços somente será possível mediante apresentação, pela CONTRATADA, de relatório de impacto contendo justificativas plausíveis, devidamente aceitas pelo BDMG, ou por interesse do BDMG, em caso de impedimento devidamente justificado que dificulte ou não permita a ativação do serviço.

Fase 3 – Recebimento definitivo

11.8. Concluída a entrega e implantação de cada serviço ou produto previsto neste Termo de Referência, o BDMG procederá à análise e à manifestação formal de aceite ou rejeição na forma e nos prazos dos subitens 4.2 a 4.3.2 da CLÁUSULA 4 – RECEBIMENTO DO OBJETO do contrato.

11.9. Na hipótese de rejeição, total ou parcial, o BDMG indicará as não conformidades identificadas, cabendo à CONTRATADA promover as correções, complementações ou ajustes necessários no prazo do subitem 4.3.1 do contrato, sem qualquer ônus adicional para o BDMG.

11.10. Após a implementação das correções, a entrega será novamente submetida à avaliação do BDMG para fins de homologação e aceite.

11.11. A fase de implantação somente será considerada concluída, e o Termo de Recebimento Definitivo (TRD) somente poderá ser emitido, após a homologação formal pelo BDMG de todos os requisitos e demais condições de aceite estabelecidos:

a) Integrações e Monitoramento

- Integração e validação das fontes de log, com evidência de coleta, recebimento, normalização e parsing correto:
    - Active Directory
    - Microsoft Entra ID
    - firewall Check Point
    - WAF Akamai
    - SentinelOne EDR/XDR
    - Microsoft Defender for Office 365
- Integração bidirecional e operacional entre o Microsoft Sentinel e a ferramenta de ITSM;
- Validação de, no mínimo, 50 casos de uso ativos no Microsoft Sentinel, com cobertura MITRE ATT&CK documentada e comparada à linha de base, entendida como o inventário de regras analíticas ativas no Microsoft Sentinel do BDMG na data da reunião inicial de alinhamento de que trata o subitem 11.2, levantado pela CONTRATADA e formalizado no Plano de Implantação;
- Validação dos playbooks, automation rules e demais mecanismos de automação, com evidências de execução;
- Publicação do conteúdo versionado no repositório Git do BDMG;
- Entrega da documentação operacional e do documento As-Built do ambiente Microsoft Sentinel.

INFORMAÇÃO CONTROLADA

b) Ferramenta de ITSM, Atendimento e Governança

- Disponibilização de acesso à ferramenta de ITSM da CONTRATADA, com SLAs configurados e testados;
- Provisionamento e homologação dos acessos nominais do BDMG;
- Entrega da matriz RACI, plano de escalonamento e demais documentos de governança;
- Testes documentados de abertura de chamados por todos os canais previstos, em horário comercial e em regime de plantão, incluindo evidências de registro, preservação dos carimbos de tempo originais e confirmação de abertura nos prazos contratuais;
- Execução dos testes de contingência dos mecanismos de coleta e dos procedimentos de acionamento do plantão.

c) Portal de Visibilidade Executiva e Operacional

- Disponibilização de acesso ao Portal de Visibilidade Executiva e Operacional com dados reais do período;
- Painéis dos subitens 9.13 a 9.17 em funcionamento, com dados reais do período;
- Perfis de acesso disponibilizados aos usuários indicados pelo BDMG;
- Exportação de dados em CSV e JSON validada diretamente pelo Banco;
- Disponibilização e documentação da API de consulta.

d) Gestão de Vulnerabilidades

- Apresentação de documentação comprobatória do licenciamento da solução de gestão de vulnerabilidades, bem como da garantia e do contrato de suporte técnico com o fabricante durante a vigência contratual
- Implantação da solução de gestão de vulnerabilidades e patch management;
- Console em produção, RBAC configurado e acessos homologados;
- Descoberta e inventário dos ativos do escopo contratado, conciliados com o inventário do BDMG;
- Execução do primeiro ciclo completo de varredura autenticada da rede interna, alcançando cobertura mínima de 98% dos ativos do escopo;
- Execução do primeiro ciclo DAST para as aplicações web relacionadas no subitem 6.4;
- Integração da solução com o Microsoft Sentinel;
- Configuração e homologação dos procedimentos de patch management, incluindo deployment rings, grupos piloto, calendários de manutenção, regras de aprovação, rollback e exceções;
- Aprovação da classificação de ativos críticos e não críticos para fins de priorização, definição de janelas de manutenção e autorização de aplicação pelas equipes do BDMG;
- Entrega do Relatório Inicial de Exposição e da linha de base de vulnerabilidades;
- Definição conjunta do escopo e do calendário inicial do ciclo de gestão de vulnerabilidades.

INFORMAÇÃO CONTROLADA

e) Capacitação e Transferência de Conhecimento

- Realização de treinamentos hands-on para a equipe de segurança do BDMG para utilização da solução de gestão de vulnerabilidades e patch management e da ferramenta de ITSM.

Fase 4 – Operação

11.12. A emissão, pelo BDMG, do Termo de Recebimento Definitivo (TRD) marcará o início da fase de prestação dos serviços de natureza continuada, a partir da qual será permitido o faturamento dos serviços pela CONTRATADA, na forma da CLÁUSULA 7 – PAGAMENTO do contrato.

11.13. A CONTRATADA entregará, até o 5º (quinto) dia útil de cada mês, relatório gerencial do mês anterior contendo, no mínimo: (a) MTTD, MTTA, MTTC e MTTR apurados por severidade; (b) taxa de falso positivo por regra analítica e consolidada; (c) percentual de alertas encerrados sem intervenção humana; (d) cobertura MITRE ATT&CK das regras ativas e variação no período; (e) volume ingerido por tabela e por fonte, custo estimado de ingestão e economias obtidas; (f) saúde de conectores e fontes silenciadas; (g) aderência a SLA por indicador e glosas apuradas; (h) situação das vulnerabilidades por severidade e prazo; e (i) plano de ação para os indicadores fora da meta.

11.14. O relatório será entregue em PDF e, obrigatoriamente, com os dados brutos que o sustentam em CSV e JSON, permitindo ao BDMG reproduzir integralmente os cálculos.

11.15. O BDMG e a CONTRATADA realizarão reuniões periódicas de acompanhamento operacional, tático e estratégico dos serviços contratados, conforme a periodicidade definida para cada instância de governança. Nessas reuniões deverão ser apresentados, no mínimo, os indicadores de desempenho e níveis de serviço (SLA), incidentes relevantes, disponibilidade dos serviços, situação dos chamados, evolução dos casos de uso, volume de ingestão de dados, vulnerabilidades críticas identificadas, resultados das campanhas de Caça a Ameaças (Threat Hunting), riscos relevantes e respectivos planos de ação.

11.16. As reuniões de governança e os relatórios gerenciais deverão utilizar exclusivamente as informações e indicadores disponibilizados no Portal de Visibilidade Executiva e Operacional, observada a rastreabilidade aos dados-fonte. É vedada a apresentação de indicadores, métricas ou resultados que não possam ser integralmente reproduzidos e auditados a partir do portal e dos respectivos dados brutos utilizados em sua apuração.

11.17. Qualquer indicador que descumpra a meta por 2 (dois) meses consecutivos ensejará análise formal de causa raiz, com plano de ação, responsável e prazo, apresentado na reunião de governança tática subsequente.

Reuniões de Acompanhamento e Governança	**Objetivos**	**Periodicidade**	**Participantes da CONTRATADA**	**Participantes do BDMG**
Estratégica	Avaliação de riscos estratégicos; Roadmap tecnológico; Evolução de maturidade;	Quadrimestral	Preposto TAM	Superintendente de TI Gestor de Segurança

INFORMAÇÃO CONTROLADA

Reuniões de Acompanhamento e Governança	Objetivos	Periodicidade	Participantes da CONTRATADA	Participantes do BDMG
	Aprovação de mudanças estruturais; Avaliação de indicadores executivos			Fiscal do contrato
Tática	KPIs; SLAs; Pendências; Plano de ação; Situação de vulnerabilidades críticas; Incidentes relevantes	Mensal	TAM Analista de Segurança Sênior Nível 3 Dedicado	Gestor de Segurança Fiscal do contrato Analista de segurança
Operacional	Backlog; Vulnerabilidades; Mudanças; Incidentes; Casos de uso; Health check das ferramentas	Semanal	Analista de Segurança Sênior Nível 3 Dedicado	Analistas de segurança

11.17-A. A CONTRATADA manterá matriz RACI formal, elaborada a partir da matriz preliminar do Plano de Implantação e aprovada pelo BDMG até a emissão do TRD, com os papéis do BDMG e da CONTRATADA, no mínimo, em:

a) monitoramento e triagem;

b) resposta a incidentes, incluindo contenção automática e ações de alto risco, na forma do item 3.9;

c) acionamento da Sala de Guerra;

d) mudanças em regras, playbooks e automações;

e) gestão de vulnerabilidades e de patches;

f) gestão de acessos;

g) comunicação com órgãos reguladores, ANPD, CSIRTs e CTIR Gov;

h) governança contratual.

11.17-B. A matriz RACI, a relação dos playbooks aprovados para contenção automática e a lista de aprovadores das ações de alto risco serão versionadas no repositório indicado pelo BDMG e revistas, no mínimo, a cada reunião de governança estratégica e sempre que houver mudança relevante no ambiente, na equipe ou nos processos.

INFORMAÇÃO CONTROLADA

11.17-C. As reuniões de governança operacional (semanal), tática (mensal) e estratégica (quadrimestral) serão registradas em ata, com as decisões, os responsáveis e os prazos, e suas pendências serão acompanhadas na ferramenta de ITSM.

11.18. Relatórios, extrações e evidências solicitados pela fiscalização do contrato ou pela área de segurança da informação do BDMG fora da periodicidade ordinária deverão ser entregues em até 5 (cinco) dias úteis contados da solicitação formal registrada na ferramenta de ITSM. Quando a solicitação decorrer de atendimento a órgão regulador, a auditoria ou a incidente em curso, o prazo será pactuado no registro da demanda e não excederá o prazo fixado pela autoridade requisitante.

12. ACORDO DE NÍVEIS DE SERVIÇO

12.1. Os Acordos de Níveis de Serviço (SLA) são parâmetros claros e mensuráveis que têm como objetivo avaliar e verificar vários aspectos dos serviços contratados, incluindo qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança. Esses critérios são estabelecidos de forma objetiva para garantir a excelência na prestação dos serviços.

12.2. O desempenho dos serviços contratados será medido por meio de SLAs e Indicadores-Chave de Desempenho (KPIs), os quais constituirão instrumentos de acompanhamento, fiscalização, aceite, aplicação de glosas, penalidades e avaliação contínua da qualidade dos serviços prestados.

12.3. A responsabilidade de cumprir os SLAs é da CONTRATADA. A avaliação será realizada pela equipe de fiscalização do BDMG mensalmente, levando em consideração as metas exigidas dos serviços, conforme as tabelas e os indicadores dos subitens 12.13 a 12.24. Para os casos de haver mais de uma ocorrência, as glosas por inadimplemento serão cumulativas, observados os limites da nota II do subitem 12.25.

12.4. Todos os indicadores deverão ser mensurados mensalmente, registrados na ferramenta de ITSM disponibilizada pela CONTRATADA e apresentados em relatórios gerenciais e executivos ao BDMG, sempre acompanhados dos dados brutos que os sustentam, admitida a recusa da medição pela fiscalização enquanto não apresentados os dados brutos correspondentes.

12.5. O descumprimento dos Níveis Mínimos de Serviço sujeita a CONTRATADA às glosas do subitem 12.25, que têm natureza de ajuste de medição e não se confundem com sanções. Sem prejuízo das glosas, sujeitam a CONTRATADA às sanções da CLÁUSULA 16 – SANÇÕES CONTRATUAIS do contrato, observados os procedimentos nela previstos: (i) o não atingimento reiterado do mesmo nível mínimo de serviço, na forma da alínea ‘a’ do subitem 16.4.1 e do subitem 16.4.2; e (ii) o resultado mensal inferior a 80% (oitenta por cento), que ensejará a abertura de processo sancionatório, na forma da tabela do subitem 12.25. A persistência do descumprimento poderá ensejar, ainda, a rescisão contratual, nas hipóteses da nota III do subitem 12.25.

12.6. As métricas MTTD, MTTA, MTTC e MTTR serão apuradas exclusivamente com base nos registros e carimbos de tempo do Microsoft Sentinel e da ferramenta de ITSM adotada na

execução contratual, prevalecendo os registros dessas plataformas para fins de cálculo de SLA, medição e auditoria.

12.7. Para assegurar objetividade, auditabilidade e isonomia: os indicadores de tempo (MTTA, MTTD, MTTC e MTTR) serão aferidos por severidade, com meta de cumprimento, aplicando-se de forma homogênea 24x7x365, independentemente do horário de acionamento. É vedada qualquer diferenciação de prazo por janela horária para incidentes de segurança. Para a apuração do MTTD, excluir-se-á a latência de ingestão e de disponibilização de dados atribuível ao fabricante da plataforma ou à fonte de origem do evento, na forma da observação do subitem 12.21, por não se encontrar sob gestão da CONTRATADA, competindo-lhe demonstrar objetivamente, a partir dos carimbos de tempo da própria plataforma, o período excluído.

12.7-A. Os indicadores de tempo terão os seguintes marcos de início e de término, que detalham as definições do subitem 1.4:

Indicador	Início do relógio	Término do relógio
MTTD	Ocorrência do evento: carimbo de tempo do evento mais antigo que compõe o alerta, na fonte de dados	Geração do alerta no Microsoft Sentinel ou, no incidente sem alerta prévio, a detecção na forma do subitem 12.7-B
MTTA	Detecção, na forma do subitem 12.7-B	Triagem: primeira ação de analista humano que assume nominalmente o incidente e registra o início da análise. Ação de automação ou de IA não encerra o MTTA
MTTC	Detecção	Contenção confirmada: execução da ação e verificação do seu efeito, com evidência no chamado (por exemplo, ativo isolado no EDR ou conta bloqueada no Entra ID)
MTTR	Detecção	Remediação validada: serviço, ativo ou ambiente restabelecido, sem indicadores de comprometimento remanescentes, com evidência no chamado

12.7-B. Considera-se detecção a geração do alerta no Microsoft Sentinel. No incidente sem alerta prévio, a detecção é a confirmação do incidente pelo analista, quando originado de Caça a Ameaças, ou o primeiro contato do BDMG em canal oficial, na forma do subitem 8.12. Nesses casos, o MTTD será apurado e reportado como tempo de permanência da ameaça no ambiente (dwell time), sem compor o indicador de MTTD do subitem 12.15 para fins de glosa.

12.7-C. A medição dos indicadores de tempo observará, ainda, as seguintes regras:

a) os carimbos de tempo serão capturados automaticamente pelo Microsoft Sentinel, pelos mecanismos de automação e pela ferramenta de ITSM, vedado o lançamento ou a alteração manual de datas e horários. Correções serão feitas somente por registro complementar justificado, preservado o registro original;

INFORMAÇÃO CONTROLADA

b) os registros adotarão o horário UTC, sincronizado com fonte de tempo confiável, com precisão de milissegundos no Microsoft Sentinel e nos mecanismos de automação, e de, no mínimo, 1 (um) segundo na ferramenta de ITSM;

c) cada ação registrada identificará o executor: analista humano, nominalmente; automação, com o playbook ou a regra e a respectiva versão; ou recurso de Inteligência Artificial Generativa, com a ferramenta e o profissional responsável pela validação humana, na forma do subitem 3.8.6;

d) a trilha de auditoria da ferramenta de ITSM será replicada, em até 15 (quinze) minutos, para o Microsoft Sentinel do BDMG, sem permissão de alteração ou de exclusão pela CONTRATADA;

e) as consultas e a memória de cálculo dos indicadores serão versionadas no repositório Git do subitem 3.5.9, e qualquer alteração dependerá de aprovação prévia do BDMG.

12.8. Clock Stop: Para fins de apuração dos indicadores MTTC e MTTR, poderá ser descontado exclusivamente, ressalvadas as hipóteses do subitem 12.9-B, o período em que a continuidade do atendimento depender de ação ou decisão de responsabilidade do BDMG, incluindo aprovações relacionadas a ativos constantes da Lista de Ativos Críticos ou dependências formalmente registradas. A suspensão do prazo deverá ser precedida de solicitação formal da CONTRATADA, registrada na ferramenta de ITSM, contendo, no mínimo, data e hora da solicitação, descrição da ação requerida, justificativa da dependência e identificação do destinatário, devendo ser comunicada simultaneamente ao BDMG por correio eletrônico corporativo e por Microsoft Teams.

12.9. O Clock Stop somente produzirá efeitos a partir da data e hora do registro formal da solicitação na ferramenta de ITSM, sendo de responsabilidade da CONTRATADA comprovar a existência da dependência, o momento de sua ocorrência e o período efetivamente sujeito à suspensão. Não serão admitidos como motivos para aplicação de Clock Stop: a) períodos noturnos, fins de semana, feriados ou qualquer restrição relacionada ao horário de atendimento, considerando que os serviços são prestados em regime 24x7; b) indisponibilidade, falha, degradação de desempenho ou limitação de ferramentas, sistemas, infraestrutura ou processos sob responsabilidade da CONTRATADA; c) insuficiência de recursos técnicos, operacionais ou humanos da CONTRATADA.

12.9-A. Não suspendem o relógio, e integram o tempo de atendimento, os escalonamentos internos entre os níveis N1, N2 e N3, equipes, gestores ou especialistas da CONTRATADA, bem como o aguardo de resposta de fabricante, fornecedor ou parceiro por ela contratado.

12.9-B. Além da hipótese do subitem 12.8, admite-se Clock Stop, com as mesmas formalidades, somente:

a) durante janela de manutenção do ambiente do BDMG, programada e aprovada pelo Banco, quando a ação de contenção ou de recuperação depender dessa janela;

b) para os incidentes gerados por exercício simulado de ataque (Red Team, Purple Team ou emulação de adversário) comunicado previamente pelo BDMG ao Gestor do SOC, com

escopo e período definidos. Os tempos desses incidentes serão medidos e registrados no relatório do exercício, sem efeito para fins de glosa. Atividade identificada fora do escopo ou do período do exercício será tratada como incidente real.

12.10. O Clock Stop constitui o único mecanismo de suspensão aplicável aos prazos dos indicadores de segurança previstos neste Termo de Referência, prevalecendo sobre quaisquer disposições conflitantes e devendo estar integralmente documentado e auditável para fins de medição, apuração de SLA e eventual aplicação de glosas.

12.11. Estabilização escalonada: a partir do recebimento definitivo, as glosas de SLA aplicam-se em 0% (dias 0–30), 50% (dias 31–60) e 100% (a partir do 61º dia), para calibração, sem prejuízo da medição e do reporte integral desde o início. A estabilização escalonada é concedida uma única vez, não se renovando nas prorrogações contratuais.

12.11-A. A CONTRATADA consolidará a linha de base dos indicadores MTTD, MTTA, MTTC e MTTR do ambiente do BDMG do 1º (primeiro) ao 30º (trigésimo) dia de operação, contados do TRD. Esse período coincide com a primeira faixa da estabilização escalonada do subitem 12.11. A linha de base será apurada somente com dados reais do Microsoft Sentinel e da ferramenta de ITSM, vedado o uso de indicadores padronizados, de médias de outros clientes ou de referências de mercado da CONTRATADA.

12.11-B. A CONTRATADA entregará o Relatório de Linha de Base até o 5º (quinto) dia útil após o término do período, contendo, no mínimo:

a) os valores apurados por severidade, com mediana e percentil 90;

b) o volume de alertas e de incidentes por severidade e por fonte de dados;

c) a latência de ingestão por fonte de dados, para os fins do subitem 12.7;

d) a proposta de relação das fontes críticas a que se refere o subitem 12.21;

e) as consultas e a memória de cálculo empregadas, na forma do subitem 12.7-C.

12.11-C. Aprovado pelo BDMG, o Relatório de Linha de Base passa a ser a referência oficial de medição e de acompanhamento da evolução dos indicadores. A linha de base não altera as metas dos subitens 12.14 e 12.15, que permanecem como limites contratuais.

12.12. É vedado à CONTRATADA recusar, postergar, descaracterizar ou reclassificar como solicitação administrativa, de rotina ou atividade de sustentação qualquer ação necessária à contenção, erradicação, mitigação ou resposta a incidente de segurança da informação com o objetivo de afastar ou reduzir a aplicação dos SLAs para incidentes.

12.13. **Classificação de Severidade**

Prioridade	Descrição
P1 - Crítica	Incidente com indisponibilidade de serviço relevante, comprometimento confirmado, ransomware, vazamento de dados ou ameaça grave em andamento
P2 - Alta	Comprometimento potencial ou degradação significativa de serviço crítico

Prioridade	Descrição
P3 - Média	Impacto moderado sem interrupção de serviço relevante
P4 - Baixa	Solicitações administrativas, dúvidas ou ocorrências sem impacto operacional relevante

12.14. **Indicador do Nível do Serviço de MDR**

Prioridade	MTTA	Escalonamento
P1	15 min	1 hora
P2	30 min	2 horas
P3	4 horas	1 dia útil
P4	1 dia útil	3 dias úteis

12.15. **KPIs**

Indicador	Meta de cumprimento mensal
Disponibilidade do Centro de Operação de Segurança (SOC 24x7)	>= 99,9%
MTTA — P1 ≤ 15 min · P2 ≤ 30 min · P3 ≤ 4 h · P4 ≤ 1 dia útil	≥ 95%
MTTD — P1 ≤ 15 min · P2 ≤ 30 min · P3 ≤ 2 h · P4 ≤ 8 h	≥ 95%
MTTC (contenção) — P1 ≤ 1 h · P2 ≤ 2 h · P3 ≤ 8 h · P4 ≤ 24 h	≥ 95%
MTTR — P1 ≤ 24 h · P2 ≤ 36 h · P3 ≤ 48 h · P4 ≤ 72 h	≥ 95%
Índice de Falso Positivo (IFP)	≤ 30% (meses 1–6); ≤ 20% (7–12); ≤ 15% (13–24); ≤ 10% (25º+)
Incidentes tratados dentro do SLA	≥ 95%
Escalonamentos realizados corretamente	≥ 98%
Relatórios entregues no prazo (até 5º dia útil)	100%
Relatórios e extrações eventuais entregues no prazo	100%
Acurácia de Classificação: percentual de incidentes cuja classificação de desfecho é confirmada na auditoria mensal por amostragem	≥ 95%
Tempo do Ciclo de Investigação — da atribuição do incidente ao veredito, por severidade, com mediana e percentil 90	Reportado mensalmente; meta pactuada a partir do 7º mês
Consistência da Contenção por Tática — desvio-padrão do MTTC apurado por tática do MITRE ATT&CK	Reportado mensalmente; meta pactuada a partir do 7º mês

Indicador	Meta de cumprimento mensal
Entregas da disciplina de Inteligência de Ameaças no prazo (subitem 3.7.10)	100%
Conversão de IoC crítico ou de relatório de inteligência em hipótese de caça ou em ajuste de detecção, no prazo (subitem 3.7.8)	≥ 95%

12.15-A. O Índice de Falso Positivo (IFP), também denominado FPR (False Positive Ratio), é o percentual de incidentes encerrados no mês como falso positivo em relação ao total de incidentes encerrados no mesmo mês. O IFP será apurado de forma consolidada, para fins da meta do subitem 12.15, e por regra analítica, para fins de calibração. A classificação está sujeita à auditoria de Acurácia de Classificação do subitem 12.17, e o incidente encerrado como positivo benigno sem justificativa técnica registrada será considerado erro de classificação.

12.15-B. A regra analítica com IFP superior a 50% (cinquenta por cento) em 2 (dois) meses consecutivos, com, no mínimo, 10 (dez) incidentes em cada mês, será calibrada pela CONTRATADA em até 10 (dez) dias úteis ou, mediante aprovação do BDMG, desativada, com registro em chamado. A desativação não poderá reduzir a cobertura MITRE ATT&CK sem detecção substituta ou aceite formal do BDMG.

12.16. Os indicadores de qualidade Acurácia de Classificação, Tempo de Ciclo de Investigação e Consistência da Contenção por Tática MITRE ATT&CK têm por finalidade avaliar a qualidade e a efetividade das atividades de investigação e resposta a incidentes, complementando os indicadores de desempenho temporal previstos anteriormente.

12.17. O indicador de Acurácia de Classificação estará sujeito à apuração de SLA e às glosas previstas no subitem 12.25 a partir da plena exigibilidade dos níveis de serviço estabelecidos neste Termo de Referência. Para fins de verificação da Acurácia de Classificação, a amostra mensal de auditoria não poderá ser inferior a 30 (trinta) incidentes ou à totalidade dos incidentes encerrados no período, quando o volume mensal for inferior a esse quantitativo.

12.18. Os indicadores de Tempo de Ciclo de Investigação e Consistência da Contenção por Tática MITRE ATT&CK serão medidos e reportados mensalmente desde o início da operação, exclusivamente para fins de acompanhamento e evolução dos serviços, sem aplicação de glosas durante os 6 (seis) primeiros meses de execução contratual.

12.19. A partir do 7º (sétimo) mês de execução, as metas para os indicadores de Tempo de Ciclo de Investigação e Consistência da Contenção serão definidas com base na série histórica acumulada dos 6 (seis) primeiros meses de operação, pelo seguinte método: para o Tempo de Ciclo de Investigação, o percentil 90 apurado por severidade no período; e para a Consistência da Contenção por Tática, o desvio-padrão correspondente ao percentil 75 do período. Sobre os valores assim apurados admite-se tolerância de 10% (dez por cento). As metas serão formalizadas por termo de pactuação firmado pela fiscalização e pelo preposto na reunião de governança tática do 7º (sétimo) mês e passarão a integrar o conjunto de indicadores de desempenho contratual, sujeitos às glosas do subitem 12.25, a partir do mês subsequente. Não

INFORMAÇÃO CONTROLADA

havendo pactuação formal, prevalecerão os valores apurados na série histórica, sem a tolerância.

12.20. **SLA do Serviço de Caça a Ameaças (Threat Hunting)**

Indicador	Meta
Campanhas estruturadas de Caça a Ameaças executadas conforme a cadência mensal	100%
Início de campanha de Caça reativa dentro do prazo	≥ 95%
Relatório de campanha entregue com hipótese, consultas KQL, achados e veredito	100%
Conversão de achado positivo ou de lacuna de visibilidade em detecção, no prazo	≥ 95%
Relatório trimestral consolidado de cobertura entregue no prazo	100%
Taxa de Incidentes Iniciados por Caça a Ameaças (HIIRR), apurada por trimestre como indicador de acompanhamento, sem glosa (subitem 3.4.8-A)	≥ 25%

12.21. **SLA do Serviço de Engenharia de Detecção e Otimização do Microsoft Sentinel**

Indicador	Meta	Observação
Latência de ingestão a alerta — fontes críticas	≤ 5 minutos em 95% dos eventos	Aferida na plataforma; excluída a latência atribuível ao fabricante
Latência de ingestão a alerta — demais fontes	≤ 15 minutos em 95% dos eventos	Idem
Detecção de fonte silenciada (log gap) e abertura de chamado	≤ 30 minutos	Responsabilidade da CONTRATADA
Início de correção de conector ou parser	≤ 4 horas úteis	Responsabilidade da CONTRATADA
Atualização de workbooks e painéis	≤ 15 minutos	Responsabilidade da CONTRATADA
Perda de eventos atribuível a falha de configuração, parser ou DCR sob gestão da CONTRATADA	Zero	Perdas atribuíveis ao fabricante ou à fonte de origem são excluídas
Entrega do plano trimestral de otimização de custo de ingestão, com oportunidades quantificadas	100%	Responsabilidade da CONTRATADA
Reporte mensal de volume e de custo por tabela e por fonte, acompanhado dos dados brutos (subitem 3.5.27)	100%	Responsabilidade da CONTRATADA
Elevação do volume ingerido acima da linha de base sem submissão prévia ao BDMG (subitem 3.5.26)	Zero	Ressalvadas as hipóteses do subitem 3.5.26

Indicador	Meta	Observação
Rendimento da Engenharia de Detecção (DEY): novas detecções particularizadas em produção no trimestre (subitem 3.5.23-A)	≥ 6 (seis) por trimestre	Apurado no relatório trimestral do subitem 3.5.23
Regra analítica com IFP acima de 50% calibrada ou desativada no prazo (subitem 12.15-B)	100%	Responsabilidade da CONTRATADA

12.22. **SLA de Automação e Resposta do Microsoft Sentinel**

Indicador	Meta
Disparo da automation rule após a criação do incidente	≤ 60 segundos
Execução de playbook após aprovação humana registrada	≤ 5 minutos
Falha de execução de playbook por erro de construção, credencial ou lógica sob responsabilidade da CONTRATADA	≤ 2%
Correção de playbook com falha recorrente	≤ 1 dia útil da terceira falha
Abertura ou espelhamento automático do incidente no ITSM	≤ 60 segundos
Cobertura de automação: percentual de incidentes com pelo menos uma ação automatizada de enriquecimento	≥ 60%, a partir do 6º (sexto) mês contado da aprovação, pelo BDMG, dos 10 (dez) playbooks exigidos até o Termo de Recebimento Definitivo
Entrega de playbooks automatizados: 10 (dez) em produção até o TRD e 2 (dois) novos ou evoluídos por trimestre	100%
Contenção automática registrada e comunicada ao BDMG com playbook, versão, regra e nível de confiança (subitem 3.9.4)	100%
Taxa de Autonomia, apoio de IA e economia de tempo dos analistas (subitem 3.9.7)	Reportado mensalmente; sem meta e sem glosa

12.23. **KPIs da Gestão de Vulnerabilidades**

Indicador	Meta
Ativos cobertos por varredura	≥ 98%
Vulnerabilidades críticas reportadas, correlacionadas ao respectivo patch e encaminhadas nos prazos do subitem 4.8 atribuíveis à CONTRATADA	≥ 95%
Vulnerabilidades altas reportadas, correlacionadas ao respectivo patch e encaminhadas nos prazos do subitem 4.8 atribuíveis à CONTRATADA	≥ 90%
Retestes (validação pós-correção) realizados nos prazos do subitem 4.8	100%
Falsos positivos	≤ 5%
Relatório Trimestral	100%
Ativos com avaliação autenticada válida	≥ 95%

INFORMAÇÃO CONTROLADA

Indicador	Meta
Vulnerabilidades em ativos expostos à internet reportadas e encaminhadas dentro do prazo do subitem 4.8	≥ 95%
Reporte de vulnerabilidade crítica ou com exploração ativa dentro do prazo	100%
Exceções e aceites de risco com aprovador nominal, prazo de validade e reavaliação no vencimento	100%
Taxa de recorrência de vulnerabilidade validada como corrigida	≤ 5%
Vulnerabilidades críticas sem reporte, sem encaminhamento formal ao BDMG ou sem exceção aprovada, nos prazos do subitem 4.8 (backlog atribuível à CONTRATADA)	zero

12.24. **KPIs do Patch Management**

Indicador	Meta
Correlação vulnerabilidade–patch e disponibilização do pacote de correção e das instruções de aplicação nos prazos do subitem 4.8	≥ 95%
Cobertura do parque	≥ 98%
Anéis de implantação, janelas de manutenção, regras de aprovação e procedimentos de reversão (rollback) mantidos homologados e testados	100%
Acompanhamento e validação (reteste) das atualizações aplicadas pelo BDMG, nos prazos do subitem 4.8	≥ 95%
Inventário atualizado	≥ 99%

12.25. **Glosas**

Resultado do SLA Mensal	Glosa
≥ 95%	Sem glosa
90% a 94,99%	2%
85% a 89,99%	5%
80% a 84,99%	10%
Inferior a 80%	20% + abertura de processo sancionatório

I. O percentual de glosa incide sobre o valor mensal do item da planilha de preços ao qual o indicador descumprido se refere, e não sobre o valor total do contrato.

II. O somatório das glosas de um mesmo mês fica limitado a 20% (vinte por cento) do valor mensal total do contrato, sem prejuízo da instauração de processo sancionatório.

III. O descumprimento do mesmo indicador por 6 (seis) meses consecutivos — isto é, por mais 3 (três) meses após o período que enseja a advertência da alínea ‘a’ do subitem 16.4.1 do contrato —, ou a aplicação da multa do subitem 16.4.2 do contrato, poderá ensejar a rescisão contratual, na forma da CLÁUSULA 17 – RESCISÃO do contrato.

IV. A glosa tem natureza de ajuste de medição por serviço não prestado no nível contratado e não se confunde com as multas da CLÁUSULA 16 – SANÇÕES CONTRATUAIS do contrato, não se aplicando bis in idem sobre o mesmo fato.

12.26. Quando um mesmo indicador descumprir a meta em meses consecutivos, a glosa será progressiva: o percentual de glosa apurado no mês será multiplicado por 1,5 (um inteiro e cinco décimos) no 2º (segundo) mês consecutivo e por 2 (dois) a partir do 3º (terceiro). Aplicam-se o limite da nota II do subitem 12.25, o subitem 11.17 e a nota III do subitem 12.25.

12.27. Para o indicador de Disponibilidade do SOC, apurado na forma do subitem 2.11, a glosa será de 1% (um por cento) do valor mensal do item 1 do quadro de itens por hora, ou fração, de indisponibilidade que exceder o limite admitido pela meta no mês. Essa glosa substitui, para esse indicador, a tabela do subitem 12.25, observados o subitem 12.26 e o limite da nota II do subitem 12.25.

12.28. O BDMG poderá contratar, a qualquer tempo, auditoria técnica independente para validar a apuração dos níveis de serviço, o cálculo das glosas e a qualidade dos serviços prestados.

12.29. A CONTRATADA franqueará ao auditor, sem custo adicional e mediante aviso prévio de 5 (cinco) dias úteis, acesso de leitura aos registros, consultas, memórias de cálculo e evidências, à ferramenta de ITSM e ao Portal de Visibilidade Executiva e Operacional, e disponibilizará seus profissionais para entrevistas. O auditor ficará sujeito às mesmas obrigações de confidencialidade da CONTRATADA.

12.30. Constatada divergência, os indicadores e as glosas serão recalculados, assegurado o contraditório, e as diferenças serão compensadas nas faturas seguintes, ainda que a medição já tenha recebido aceite definitivo. A alteração indevida de registros sujeita a CONTRATADA às sanções contratuais.

13. PAGAMENTO

13.1. As condições de faturamento e de pagamento constam da CLÁUSULA 7 – PAGAMENTO do contrato, que disciplina a remuneração mensal dos itens 1 e 2 do quadro de itens do subitem 1.1, o pagamento em parcela única do item 3 e a ausência de remuneração do escopo de implantação, observado o recebimento disciplinado na CLÁUSULA 4 – RECEBIMENTO DO OBJETO.

14. TRANSIÇÃO CONTRATUAL

14.1. Ao término, rescisão ou não renovação contratual, a CONTRATADA executará handover técnico assistido, contemplando documentação As-Built, regras analíticas em KQL, hunting queries, parsers e funções, playbooks e automation rules, workbooks e dashboards, watchlists, runbooks, linhas de base de comportamento, modelos de aprendizado de máquina treinados sobre dados do BDMG, relatórios, evidências e sessão de transferência de conhecimento, em formatos abertos (ARM/Bicep/JSON, KQL, CSV) e no repositório Git indicado pelo BDMG.

14.2. Todo o conteúdo produzido na execução contratual, bem como os dados e logs do Microsoft Sentinel são de propriedade exclusiva do BDMG, permanecem em seu ambiente durante e

após a vigência e não podem ser removidos, desabilitados, ofuscados ou condicionados a qualquer pagamento adicional.

14.3. O período de transição assistida será de até **60 (sessenta) dias**, prorrogável uma vez por igual período a critério do BDMG, mantidas as condições contratuais e a remuneração proporcional.

14.4. Encerrada a transição, a CONTRATADA revogará em até 5 (cinco) dias úteis todos os acessos nominais, contas convidadas, delegações Azure Lighthouse, chaves de API e contas de serviço, apresentando evidência formal da revogação e da eliminação de cópias de dados do BDMG em seu ambiente, ressalvadas obrigações legais de retenção.

14.5. Os dados do BDMG mantidos em plataformas fornecidas ou operadas pela CONTRATADA — em especial a ferramenta de ITSM e os repositórios de evidências — serão preservados por, no mínimo, 90 (noventa) dias contados do término da vigência ou da rescisão contratual, de modo que possam ser integralmente extraídos e transferidos ao BDMG ou a outro prestador por ele designado, em formatos abertos e legíveis por máquina (CSV, JSON e PDF), sem custo adicional e sem condicionamento a qualquer pagamento.

14.6. Mediante autorização expressa e por escrito do BDMG, e somente após a confirmação da extração completa de que trata o subitem anterior, todos os dados do Banco, inclusive os replicados para fins de cópia de segurança, serão eliminados pela CONTRATADA em conformidade com as técnicas descritas na publicação NIST SP 800-88 (Guidelines for Media Sanitization), ou norma que venha a substituí-la, com apresentação de relatório de eliminação e de declaração assinada por representante legal, ressalvadas exclusivamente as hipóteses de guarda obrigatória por força de lei ou de norma regulamentar, que serão discriminadas, justificadas e mantidas sob as mesmas obrigações de sigilo.

14.7. A CONTRATADA prestará, sem ônus adicional, toda a assistência técnica necessária ao BDMG para a transferência dos serviços, dos dados, das configurações e do conhecimento a outro prestador que o Banco venha a designar, inclusive respondendo a questionamentos técnicos do novo prestador durante o período de transição assistida previsto.

Documento assinado digitalmente
gov.br
EVANDRO DOLABELLA MELO
Data: 06/11/2026 16:29:39-0300
Verifique em https://validar.iti.gov.br

INFORMAÇÃO CONTROLADA