CASA DA MOEDA DO BRASIL

EDITAL CMB PREGÃO ELETRÔNICO

(Processo Administrativo n.º 18750.002778/2025-01)

SEELC – Seção de Editais e Licitações

DEGEC – Departamento de Contratações

DIGES – Diretoria de Gestão

PREGÃO ELETRÔNICO Nº 90035/2026

(Processo Administrativo n.° 18750.002778/2025-11)

Torna-se público, para conhecimento dos interessados, que a CASA DA MOEDA DO BRASIL, por meio do Departamento de Contratações, sediado(a) na Rua René Bittencourt n.º 371, Distrito Industrial de Santa Cruz, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, **do tipo menor preço global, pelo modo de disputa aberto,** nos termos da Lei Federal 14.133, de 1º de abril de 2021, bem como instruções normativas que a regulem, aplicáveis exclusivamente ao procedimento da licitação e no que for compatível com o Regime das Estatais, Lei Federal nº 13.303, de 30 de junho de 2016, Decreto Federal nº 8.945, de 27 de dezembro de 2016, Lei Complementar nº 123, de 14 de dezembro de 2006, Lei Federal nº 13.709, de 14 de agosto de 2018, Decreto Federal nº 8.538, de 06 de outubro de 2015, do Decreto nº 7.174, de 12 de maio de 2010, Regulamento de Licitações e Contratos da CMB e das condições estabelecidas neste Edital e seus anexos.

Data da sessão: **26/11/2026**

Horário: **10:00H**

Local: Portal de Compras do Governo Federal – www.gov.br/compras/pt-br/

Unidade Compradora: 179083

1. DO OBJETO

1.1 O objeto da presente licitação é a prestação de **Serviço Gerenciado de Segurança (Managed Security Services - MSS) com fornecimento de soluções tecnológicas de cibersegurança**, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2 No caso de haver divergência entre a descrição constante na “Descrição Detalhada do Objeto Ofertado” no sistema do Portal de Compras do Governo Federal e aquela contida no Edital, prevalecerá sempre a descrição contida no Edital.

2. DO CREDENCIAMENTO

2.1 O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

2.2 O cadastro no SICAF poderá ser iniciado pela licitante no Portal de Compras do Governo Federal, no sítio www.gov.br/compras/pt-br/, com a solicitação de login e senha pelo interessado.

2.3 O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

2.4 A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.

2.5 O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.6 Cabe à licitante acompanhar as operações no sistema eletrônico durante a sessão pública, ficando responsável pelo ônus decorrente da perda de negócios em razão de sua própria desconexão ou diante da inobservância de qualquer mensagem emitida pelo sistema.

2.7 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.7.1 A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

3. DA PARTICIPAÇÃO NO PREGÃO

3.1 Poderão participar deste Pregão empresas interessadas cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular

no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme Instrução Normativa SEGES/MPOG n.º 3, de 2018.

3.1.1 Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

3.2 Cada representante somente poderá representar uma única licitante na disputa de cada item, lote ou grupo.

3.3 Não poderão participar desta licitação os interessados que:

I. se enquadrem em alguma das vedações previstas na legislação, especialmente na Lei nº 13.303, de 2016, notadamente em seu artigo 38, bem como na Lei n° 14.133, de 2021, notadamente em seu artigo 14;

II. estejam sob falência ou em processo de dissolução;

III. estejam em recuperação judicial, salvo se amparada em certidão emitida pela instância judicial competente, que certifique que a interessada está apta econômica e financeiramente a participar de procedimento licitatório (Acórdãos nºs 8.271/2011 – 2ª câmara e 1201/2020 – Plenário);

IV. estejam cumprindo penalidade de suspensão temporária de participação em licitação e impedimento de contratar com o CMB;

V. tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública ou estejam cumprindo penalidade de impedimento de licitar e contratar com a União Federal;

VI. estejam proibidos de licitar e contratar com a Administração Pública bem como de receber incentivos, subsídios, subvenções, doações ou empréstimos de pessoas jurídicas de direito público ou de pessoas jurídicas controladas pelo Poder Público, com fundamento em outros dispositivos de leis esparsas;

VII. possuam em seu contrato ou estatuto social finalidade ou objetivo incompatível com o objeto deste Pregão;

VIII. estejam organizados sob a forma de consórcio;

IX. mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente da CMB ou com agente público que

desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

3.4 Será permitida a participação de sociedades optantes do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e das Empresas de Pequeno Porte – Simples Nacional, observadas as orientações dispostas nos subitens a seguir.

3.4.1 Não são aplicáveis os benefícios e demais disposições previstas nos artigos 42 a 49 da Lei Complementar nº 123, de 2006 no caso de licitação para aquisição de bens ou contratação de serviços em geral, ao item e, em se tratando de contratação de obras e serviços de engenharia, às licitações cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

3.4.1.1 A obtenção dos benefícios fica limitada às microempresas e às empresas de pequeno porte que, no ano calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

3.4.1.2 Nas contratações com prazo de vigência superior a 1 (um) ano, será considerado o valor anual do contrato.

3.4.2 O Licitante optante do Simples Nacional que vier a executar atividade vedada pelo artigo 17 da Lei Complementar nº 123, de 2006, não poderá beneficiar-se da condição de optante.

3.4.2.1 Na hipótese do subitem anterior deste Edital, uma vez celebrado o instrumento de contratação, o Contratado deverá providenciar, perante a Receita Federal do Brasil – RFB, sua exclusão obrigatória do Simples Nacional, no prazo estipulado pelo artigo 30 da Lei Complementar nº 123/2006.

3.4.3 O Licitante optante do Simples Nacional, que não se enquadre em situação de vedação prevista no artigo 17 da Lei Complementar nº 123/2006, somente poderá beneficiar-se de tal condição se, com o valor ofertado em sua proposta, não vier a exceder o limite de receita bruta anual, previsto no artigo

3º da Lei Complementar nº 123, de 2006, ao longo da vigência do instrumento de contratação.

3.4.3.1 Se o Licitante optante do Simples Nacional extrapolar o limite de receita bruta anual previsto no artigo 3º da Lei Complementar nº 123, de 2006 ao longo da vigência do instrumento de contratação, uma vez sendo contratado deverá providenciar, perante a Receita Federal do Brasil – RFB, sua exclusão obrigatória do Simples Nacional, no prazo estipulado pelo artigo 30 da Lei Complementar nº 123, de 2006.

3.4.4 Não serão aceitos pedidos de reequilíbrio econômico-financeiro do instrumento de contratação fundamentados na alteração de regime tributário decorrente dos itens 3.4.1.1 e 3.4.2.1 deste Edital, devendo o Contratado arcar com eventuais custos decorrentes desta alteração.

3.5 Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

3.5.1 que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

3.5.1.1 nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

3.5.1.2 nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.5.2 que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021, no caso de licitante organizado em cooperativa;

3.5.3 que está ciente e concorda com as condições contidas no Edital e seus anexos;

3.5.4 que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

3.5.5 que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

3.5.6 que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

3.5.7 que a proposta foi elaborada de forma independente;

3.5.8 que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.5.9 que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

3.5.10 que cumpre os requisitos do Decreto nº 7.174/2010, estando apto a usufruir dos critérios de preferência.

3.6 A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às consequências e sanções previstas em lei e neste Edital.

4. DA APRESENTAÇÃO DA PROPOSTA E DOS LANCES

4.1 Na presente licitação a fase de habilitação sucederá as fases de apresentação de propostas, lances e de julgamento.

4.2 As licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital e seguindo-se o modelo do Anexo II, até a data e o horário estabelecidos para a abertura da sessão pública.

4.2.1 Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema.

4.2.2 Todas as especificações do objeto contidas na proposta vinculam o fornecedor registrado.

4.2.3 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.2.4 O prazo de validade da proposta não será inferior a **60 (sessenta) dias**, a contar da data de sua apresentação.

4.3 O cadastro da proposta no sistema implica a aceitação integral e irretratável dos termos do presente Edital, não sendo admitidas alegações de erros, omissões ou desconhecimento de fatos e de condições que impossibilitem ou dificultem a execução do objeto licitado.

4.4 A licitante declarada vencedora do certame deverá enviar a proposta de preços, conforme subitem 4.2 deste Edital, de acordo com o formulário que segue como Anexo II deste Edital, com todas as informações e declarações ali constantes, devendo ser redigida em língua portuguesa, no papel timbrado da empresa, com clareza, perfeitamente legível, sem emendas, rasuras, borrões, acréscimos, ou entrelinhas, sendo datada e assinada digitalmente (por certificado digital) por seu representante legal ou procurador constituído, devidamente identificado com números de CPF e RG, e respectivo cargo na licitante.

4.5 O envio da proposta ocorrerá por meio de chave de acesso e senha.

4.6 Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de abertura da sessão pública e da fase de envio de lances.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1 Na data e no horário de abertura da sessão pública o sistema a abrirá automaticamente, sem qualquer ingerência do Pregoeiro.

5.2 Incumbirá à licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.3 O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

5.4 O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.5 Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.6 Os lances serão ofertados pelo **menor preço global**, devendo a licitante após a negociação e na contratação apresentar as planilhas de composição de custos unitários do serviço licitado.

5.7 O licitante somente poderá oferecer **lance inferior** ao último por ele ofertado e registrado pelo sistema.

5.7.1 A licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 (quinze) segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.7.1.1 **lance inconsistente:** aquele cujo valor seja incoerente em relação à quantidade ou à qualidade do item licitado; e

5.7.1.2 **lance inexequível:** aquele que represente preço simbólico, irrisório ou igual a zero.

5.7.2 O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 1,00 (um real)

5.7.3 O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a 20 (vinte) segundos e o intervalo entre lances não poderá ser inferior a 3 (três) segundos.

5.8 Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.9 Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.10 Para o envio de lances na sessão pública será adotado o modo de disputa “aberto”, em que os licitantes apresentarão lances públicos e sucessivos.

5.10.1 A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

5.10.2 A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.10.3 Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

5.10.4 Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o Pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para definição das demais colocações.

5.10.5 Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

5.11 No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.12 Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.13 Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.14 Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 34 da Lei nº 11.488, de 2007, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006, bem como para bens e serviços produzidos no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.

5.15 Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema

identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.16 Nessas condições, as propostas de microempresas, empresas de pequeno porte e sociedades cooperativas que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.17 A licitante melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.18 Caso a microempresa, empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa, empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito.

5.19 No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.20 Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

5.20.1 Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

5.20.1.1 bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

5.20.1.2 bens e serviços com tecnologia desenvolvida no País; e

5.20.1.3 bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

5.20.2 Os licitantes classificados que estejam enquadrados no item 5.24.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

5.20.3 Caso a preferência não seja exercida na forma do item 5.24.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 5.24.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 5.24.1.3 caso esse direito não seja exercido.

5.20.4 As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

5.21 Somente poderá haver empate entre propostas iguais não seguidas de lances, ou entre lances finais da fase fechada do modo de disputa “aberto e fechado”.

5.21.1.1 Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 55 da Lei 13.303/2016 c/c art. 60 da Lei nº 14.133, de 2021, de acordo com a ordem legalmente estabelecida. A permanecer o empate, o sorteio eletrônico será aplicado, como critério derradeiro.

5.22 O Pregoeiro se reserva o direito de excluir as propostas ou os lances simbólicos, irrisórios, de valor zero ou considerados manifestamente inexequível, que possam comprometer, restringir ou frustrar o caráter competitivo do processo licitatório.

5.22.1 Caso não concorde com a exclusão, a Licitante poderá manter sua proposta e eventuais lances e reingressar à fase de disputa.

5.22.2 A exclusão do lance não impedirá a continuidade do envio de lances pelos fornecedores.

5.23 Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar contraproposta à licitante que tenha apresentado o melhor preço, para

que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

5.23.1 A negociação poderá ocorrer, entre outras hipóteses, quando a proposta da primeira colocada não atender ao critério de aceitabilidade relacionado ao preço.

5.23.2 Quando a primeira colocada, mesmo após a negociação, for desclassificada em razão de sua proposta permanecer acima do preço máximo estimativo da contratação, a negociação poderá ser feita com as demais licitantes, respeitada a ordem de classificação estabelecida

5.24 O Pregoeiro solicitará à licitante mais bem classificada que, no prazo mínimo de **2 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares.

5.24.1 É facultado ao Pregoeiro prorrogar o prazo estabelecido, em função da complexidade envolvida na preparação e/ou do envio da proposta ou a partir de solicitação fundamentada feita pela licitante, antes de findo o prazo, devendo informar a referida providência no chat da licitação.

5.25 A fim de verificar a pertinência de declaração de enquadramento da licitante mais bem classificada como microempresa ou empresa de pequeno porte, o Pregoeiro realizará consulta ao Portal da Transparência do Governo Federal (www.portaldatransparencia.gov.br) para verificar se o somatório de ordens bancárias recebidas pela licitante ME-EPP, relativas ao último exercício e ao exercício corrente, até o mês anterior ao da data de abertura do certame extrapola o limite máximo de faturamento previsto no art. 3º da Lei complementar nº 123, de 2006.

5.25.1 Constatado, a partir da verificação de que trata o subitem anterior, que o volume de ordens bancárias recebidas pela licitante supera o limite previsto no inciso II do art. 3º da Lei Complementar nº 123, de 2006, o Pregoeiro relatará o fato em campo próprio no sistema e concederá à respectiva licitante a oportunidade de manifestação acerca da matéria, com vistas a, eventualmente, demonstrar a adequação de sua declaração de enquadramento como ME/EPP.

5.25.2 Aplica-se o disposto no subitem anterior caso seja constatado, de ofício pelo Pregoeiro ou mediante provocação de terceiro, que a licitante esteja

contemplada em uma das hipóteses previstas no § 4º do art. 3º da Lei Complementar nº 123, de 2006 ou, ainda, tenha celebrado no ano-calendário de realização da licitação.

6. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

6.1 Encerrada a etapa de lances, o pregoeiro examinará a proposta classificada em primeiro lugar realizando a verificação de sua conformidade quanto à sua adequação ao objeto, observados os requisitos, as especificações técnicas e os parâmetros definidos neste Edital e seus anexos, e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

6.1.1 Será considerada vencedora do certame licitatório a licitante que apresentar o menor preço global resultante da planilha de preços constantes do ANEXO II.

6.1.1.1 Não será considerada qualquer oferta de vantagem não prevista neste Edital e em seus Anexos.

6.2 A proposta comercial apresentada deverá ser elaborada em língua portuguesa (Brasil), com suas páginas numeradas, sem emendas, acréscimos, borrões, rasuras, ressalvas, entrelinhas ou omissões que acarretem lesão ao direito dos demais licitantes, prejuízo à CMB ou impeçam a exata compreensão de seu conteúdo. A proposta deverá contar, no mínimo, com os seguintes elementos:

6.2.1 Razão social, CNPJ, endereço completo, número de telefone e correio eletrônico (e-mail) do licitante;

6.2.2 Valores expressos em Real (R$), observando o número máximo de 02 (duas) casas decimais após a vírgula;

6.2.3 Data e assinatura do representante do licitante, com a identificação de seu nome abaixo da assinatura;

6.2.4 Prazo de validade da proposta (mínimo de sessenta dias), a contar da data da sessão pública.

6.3 A proposta deverá apresentar, de forma clara, completa e detalhada, a especificação dos valores mensais individuais e totais referentes aos serviços executados pelo licitante, bem como de cada componente da solução tecnológica a ser fornecido (hardware, software, licenças, assinaturas, etc.), incluindo ao menos as seguintes informações:

6.3.1 Nome e modelo do componente da solução;

6.3.2 Nome do fabricante;

6.3.3 Part Number (código de identificação única do fabricante);

6.3.4 Forma de fornecimento (on-premise, Data Center próprio do licitante, Data Center de terceiros alocado pelo licitante, Data Center de provedores de cloud públicas de mercado ou Data Center do próprio fabricante);

6.3.5 Quantidade e unidade/métrica utilizada;

6.3.6 Valor unitário mensal do componente;

6.3.7 Valor total mensal do componente (Quantidade × Valor unitário);

6.3.8 Valor do Subtotal mensal correspondente da solução.

6.4 A proposta deverá ser complementada por planilha “ponto a ponto” de comprovação do atendimento dos requisitos técnicos previstos neste instrumento, em conformidade com modelo constante em **“Comprovação de Requisitos” (APENSO G)** do Termo de Referência;

6.4.1 Para sua devida comprovação, além dos requisitos específicos já destacados diretamente no **APENSO G**, caberá à CONTRATADA apresentar também comprovação de todos os requisitos técnicos exigidos para as soluções tecnológicas ofertadas;

6.4.2 Para o correto preenchimento do documento disponibilizado no **APENSO G**, o proponente deverá tomar como base a seguinte orientação atinente às colunas da planilha:

I. **ITEM:** Deve ser indicado o número do item vinculado ao requisito técnico exigido, em consonância com o disposto na seção **“Soluções Tecnológicas de Cibersegurança”** presente na **"Especificação Técnica" (APENSO A)** do Termo de Referência. Todos os itens devem ser obrigatoriamente listados para sua devida comprovação. Caso o licitante entenda que algum item não seja passível de comprovação, deverá apresentar justificativa razoável/plausível na coluna “observação”, sujeita a apreciação e eventual aceitação por parte da CMB;

II. **DOCUMENTO:** Deve ser indicado o nome do documento enviado pelo proponente, que contém o conteúdo comprobatório do requisito exigido. Este documento será utilizado pela CMB para averiguação da conformidade. Portanto, visando evitar possíveis falhas interpretativas e agilizar o processo de avaliação, recomenda-se que o proponente

adote uma padronização de nomes clara e consistente para os documentos apresentados;

III. **PÁGINA:** Deve ser indicado o número da página do documento que contém o conteúdo comprobatório do requisito técnico;

IV. **TRECHO:** Deve ser destacado, sem modificações (ipsis litteris), segmento do texto original presente do documento oficial que comprove o atendimento satisfatório do requisito técnico exigido;

V. **OBSERVAÇÃO:** Deve ser indicado qualquer informação relevante ou complementar que possa auxiliar a CMB na correta compreensão do conteúdo comprobatório apresentado pelo licitante. Além disso, deve ser utilizado para apresentação de justificativa em caso de impossibilidade de comprovação.

6.4.3 Para fins de comprovação dos requisitos técnicos, os seguintes documentos oficiais do fabricante, relativos às soluções tecnológicas ofertadas, poderão ser apresentados:

I. Datasheet ou especificações técnicas oficiais;

II. Guia de implementação ou manual de configuração;

III. Documento de arquitetura da solução;

IV. Notas de versão (release notes) da versão mais recente;

V. Whitepaper técnico detalhando as funcionalidades principais;

VI. Documentação de API (se aplicável);

VII. Certificações relevantes do produto;

VIII. Documento de comparativo técnico com soluções similares;

IX. Artigos técnicos publicados em blog oficial do fabricante.

6.4.4 A documentação técnica poderá, caso necessário, ser disponibilizada por meio de repositório eletrônico próprio (Ex. Microsoft OneDrive, Google Drive, etc.), desde que sejam devidamente informados a URL completa, a senha de acesso (se aplicável) e assegurado que a permissão para download dos arquivos esteja ativa para a CMB;

6.4.5 Todos os documentos comprobatórios apresentados deverão ser oficiais do fabricante, não sendo aceito documentos de terceiros;

6.4.6 Não serão aceitas declarações ou cartas de conformidade ou adequação ao especificado no Termo de Referência em substituição ou complementação da documentação oficial do fabricante;

6.4.7 Serão aceitos apenas documentos em português, inglês ou espanhol para comprovação das especificações técnicas.

6.5 O fornecimento das soluções deverá englobar todos os hardwares, softwares e licenças necessários ao seu funcionamento e para o pleno atendimento das especificações técnicas exigidas, mesmo que não solicitados explicitamente neste Termo de Referência;

6.5.1 Caso o licitante necessite fornecer hardwares e/ou softwares adicionais não especificados nominalmente, mas necessários para o atendimento das funcionalidades exigidas, estes deverão estar devidamente identificados na proposta, juntamente com seus custos individuais.

6.6 A entrega dos documentos previstos nesta seção é obrigatória, tendo o objetivo de garantir a correta identificação do objeto ofertado pelo proponente. Tal exigência visa permitir à CMB uma avaliação precisa das propostas, assegurando sua integral aderência aos requisitos estabelecidos, além de prevenir a ocorrência de sobrepreços, superfaturamento ou a inclusão indevida de custos que possam resultar em pagamentos irregulares, conforme previsto no Art. 31 da Lei nº 13.303/2016;

6.6.1 A **não conformidade da proposta comercial**, seja por ausência ou inadequação aos padrões estabelecidos, poderá resultar na **desclassificação do licitante.**

6.7 A CMB poderá promover diligências diretamente com o licitante para dirimir quaisquer dúvidas, esclarecer ou complementar informações apresentadas a fim de aferir a sua veracidade, o que poderá ocorrer, a seu critério, de forma presencial, audioconferência ou e-mail

6.8 Será desclassificada a proposta:

6.8.1 que contenha vício(s) insanável(is);

6.8.2 com valor superior ao valor estimado;

6.8.3 que apresentar preço manifestamente inexequível;

6.8.4 não apresentarem as especificações técnicas exigidas pelo Termo de Referência ou projeto básico, inclusive às relacionadas à marca e/ou modelo, conforme documento Recomendação Técnica ou Justificativa Técnica, assinalados como únicos capazes de atender o objeto do contrato; ou

6.8.5 Não corrigir ou não justificar eventuais falhas apontadas pelo Pregoeiro(a).

6.9 Considera-se inexequível a proposta que apresente preços simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade da licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.

6.10 A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio da Planilha de Custos e Formação de Preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme anexo deste Edital.

6.11 A Planilha de Custos e Formação de Preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de mínimo de 2 (duas) horas, contado da solicitação do pregoeiro, com os respectivos valores readequados ao lance vencedor, e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

6.12 A inexequibilidade dos valores referentes a itens isolados da Planilha de Custos e Formação de Preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

6.13 Havendo indícios de inexequibilidade do(s) valor(es) ofertado(s) ou custo(s) que compõe(m) a proposta, será instaurada diligência para que o Licitante ofertante da melhor proposta possa, no prazo fixado pelo Pregoeiro:

6.13.1 comprovar sua exequibilidade; ou

6.13.2 ajustar o(s) custos(s) orçados(s), apresentando planilha de preço readequada, respeitando, em todo caso, o valor da sua proposta (Acórdão 2.546/2015 – Plenário e 7618/2020 - TCU – 1ª Câmara), com as respectivas justificativas para o(s) ajuste(s) realizado(s).

6.13.2.1 Optando por comprovar a exequibilidade de sua proposta, o Licitante deverá apresentar justificativas e documentos que comprovem a viabilidade e a compatibilidade do(s) valor(es) e custo(s) ofertados com os custos e despesas necessários à integral execução do objeto.

6.14 O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo mínimo de **2 (duas) horas**, sob pena de não aceitação da proposta.

6.14.1 Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se as planilhas de custo readequadas com o valor final ofertado.

6.14.2 O prazo estabelecido pelo Pregoeiro poderá ser prorrogado de ofício ou por solicitação escrita e justificada do licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.

6.14.3 Para a contagem de prazo de trata o item anterior não será considerado o tempo de eventual suspensão da sessão pública realizada pelo Pregoeiro.

6.15 Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

6.15.1 O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

6.15.2 Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

6.16 Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, inclusive negociando os valores, e, assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este Edital.

6.17 Sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

6.18 Na hipótese de necessidade de suspensão da sessão pública, inclusive para a realização de diligências, o Pregoeiro informará a data e horário de retorno ou, no caso de impossibilidade, a reiniciará mediante aviso prévio no sistema com, no mínimo, **24 (vinte e quatro) horas** de antecedência.

6.19 Encerrada a análise quanto à aceitação da proposta, o Pregoeiro passará à fase de **verificação da habilitação do licitante**, observado o disposto neste Edital.

7. DA HABILITAÇÃO

7.1 Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual

descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1 SICAF;

7.1.2 Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (https://www.transparenciapublica.gov.br/);

7.1.3 Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

7.1.4 Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/)

7.1.5 A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

7.1.6 Caso conste na Consulta de Situação da licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para o levantamento de conjunto de indício, analisando eventual configuração da tentativa de fraude ou burla ao sancionamento por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

7.1.6.1 A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, data de constituição da nova empresa posterior à data de aplicação da sanção/impedimento ou declaração de inidoneidade, compartilhamento ou transferência da mesma estrutura física, técnica ou de recursos humanos, identidade (ou proximidade) de endereço dos estabelecimentos, identidade de telefones, e-mail's, contadores e demais informações de contrato, dentre outros.

7.1.6.2 Diante da presença de um conjunto convergente de indícios referidos nos subitens anteriores, o Pregoeiro registrará, no *chat,* as ocorrências levantadas, suspenderá o certame e oportunizará à

licitante o exercício do contraditório e ampla defesa, devendo a licitante apresentar todos os esclarecimentos e documentação tendentes a ilidir a suspeita da prática de comportamento ilícito.

7.1.7 Constatada a existência de sanção ou a tentativa de fraude ou burla dos efeitos de sanção aplicada a outra empresa, o Pregoeiro (I) reputará a licitante inabilitada, por falta de condição de participação e (II) relatará o fato à autoridade competente para instauração de procedimento administrativo específico objetivando a apuração exauriente acerca dos fatos e eventual responsabilização da licitante pela prática de comportamento inidôneo.

7.2 O Pregoeiro poderá consultar o Sistema de Cadastro Unificado de Fornecedores – SICAF, em relação à habilitação jurídica, técnica, fiscal, social e trabalhista, e econômico-financeira, conforme disposto no artigo 39 da Instrução Normativa SEGES/ME n.º 73, de 2022.

7.2.1 Também poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando o licitante esteja com alguma documentação vencida junto ao SICAF.

7.2.2 Caso o Pregoeiro não logre êxito em obter a certidão correspondente através do sítio oficial, ou na hipótese de se encontrar vencida no referido sistema, o licitante será convocado a encaminhar, no prazo mínimo de 48 (quarenta e oito) horas, documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação, ressalvado o disposto quanto à comprovação da regularidade fiscal das microempresas, empresas de pequeno porte e das sociedades cooperativas, conforme estatui o art. 43, § 1º da LC nº 123, de 2006, regulamentado pelo Decreto nº 8.538/2015.

7.3 Os licitantes que não estiverem cadastrados no Sistema de Cadastro Unificado de Fornecedores – SICAF além do nível de credenciamento exigido pela Instrução Normativa SEGES/MPOG n.º 3, de 2018 deverão apresentar a seguinte documentação de habilitação, após solicitação do Pregoeiro:

7.3.1 Habilitação jurídica:

7.3.1.1 No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

7.3.1.2 No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo em vigor,

devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

7.3.1.3 No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

7.3.1.4 No caso de microempresa ou empresa de pequeno porte: certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte nos termos da IN DREI nº 10/2013;

7.3.1.5 No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

7.3.1.6 No caso de sociedade estrangeira em funcionamento no país, Decreto de autorização e, quando a atividade assim o exigir, Ato de registro ou Autorização para funcionamento expedido pelo órgão competente.

7.3.1.7 No caso de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI;

7.3.1.8 Todos os documentos acima devem estar acompanhados de todas as alterações ou da consolidação respectiva;

7.3.2 Regularidade fiscal, social e trabalhista:

7.3.2.1 Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

7.3.2.2 Certidão Conjunta Negativa de Débitos relativos a Tributos e Contribuições Federais pela Secretaria da Receita Federal do Brasil (SRFB) e as inscrições em Dívida Ativa da União junto a Procuradoria-Geral da Fazenda Nacional (PGFN), na forma da Portaria Conjunta RFB/PGFN nº 1.751, de 02/10/2014 do domicílio ou sede da licitante;

7.3.2.3 prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

7.3.2.4 as licitantes deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, sob pena de inabilitação.

7.3.3 Qualificação econômico-financeira:

7.3.3.1 Os licitantes que não estiverem cadastrados no Sistema de Cadastro Unificado de Fornecedores - SICAF no **nível da Qualificação econômico-financeira**, conforme Instrução Normativa SEGES/MPOG n.º 3, de 2018, deverão apresentar a seguinte documentação:

7.3.3.1.1 Certidão negativa de falência ou recuperação judicial expedida pelo distribuidor da sede da pessoa jurídica;

7.3.3.1.1.1 A licitante poderá substituir a certidão negativa de recuperação judicial pela certidão emitida pela instância judicial competente, certificando que a interessada está apta econômica e financeiramente a participar de procedimento licitatório.

7.3.3.1.2 balanço patrimonial e demonstrações contábeis dos 2 (dois) últimos exercícios sociais, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

7.3.3.1.2.1 Serão considerados aceitos como na forma da lei o balanço patrimonial e demonstrações contábeis assim apresentados:

7.3.3.1.2.1.1 sociedades regidas pela Lei nº 6.404/76: publicados em Diário Oficial, ou em jornal de grande circulação;

7.3.3.1.2.1.2 sociedades de grande porte, nos termos do artigo 3º da Lei nº 11.638/07, deverão seguir as disposições da Lei nº 6.404/76; (vide subitem acima)

7.3.3.1.2.1.3 outras formas societárias: por fotocópia das páginas correspondentes do Livro Diário, devidamente autenticadas na Junta Comercial ou outro órgão equivalente do Registro de Comércio da sede ou domicílio da licitante, com os competentes Termos de Abertura e Encerramento.

7.3.3.1.3 Das empresas constituídas no exercício social será exigida a apresentação de fotocópia do balanço de abertura, devidamente registrado na Junta Comercial, ou de fotocopiado Livro Diário contendo o balanço de abertura, inclusive com os termos de abertura e encerramento, devidamente registrados ou autenticados na Junta Comercial da sede ou domicílio da licitante.

7.3.3.1.4 O balanço patrimonial e as demonstrações contábeis deverão estar assinados por Contador ou por profissional equivalente, devidamente registrado no Conselho Regional de Contabilidade e pelo Titular ou representante legal da empresa LICITANTE.

7.3.3.1.5 Caso a licitante seja cooperativa, tais documentos deverão ser acompanhados da última auditoria contábil-financeira, conforme dispõe o artigo 112 da Lei nº 5.764, de 1971, ou de uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador;

7.3.3.1.6 As empresas sujeitas à apresentação da Escrituração Contábil Digital (ECD) nos termos do art. 2º do Decreto Federal nº 6.022/2007, com a utilização do Sistema Público de Escrituração Digital (SPED) deverão apresentar, o Balanço Patrimonial, a Demonstração de Resultado, os Termos de Abertura e Encerramento do livro digital.

7.3.3.1.6.1 Em se tratando de licitação para fornecimento de bens para entrega inferior a 30 dias, não se exigirá da microempresa ou empresa de pequeno porte a apresentação de balanço patrimonial do último exercício social;

7.3.3.1.7 Poderão ser apresentados balanços intermediários, desde que sua emissão seja autorizada pelo estatuto social da licitante ou decorrer de Lei.

7.3.3.1.8 A comprovação da situação financeira da licitante será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1, resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}};$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}};$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}; \text{ e}$$

7.3.3.1.9 As licitantes, cadastradas ou não no SICAF, quando o resultado de qualquer um dos índices de Liquidez Geral (LG), ou Solvência Geral (SG), ou Liquidez Corrente (LC), foi igual ou inferior a 1, deverão comprovar patrimônio líquido com valor correspondente a 10% (dez por cento) do valor da proposta.

7.3.4 **Qualificação Técnica**

7.3.4.1 As empresas, cadastradas ou não no SICAF, deverão comprovar, ainda, a qualificação técnica, por meio de:

7.3.4.1.1 Atestado de capacidade técnica, expedido por pessoa (s) Jurídica (s) de direito público ou privado que, na condição de

cliente(s) final(s), comprove(m) o fornecimento satisfatório, pela licitante, de serviço com características compatíveis com o objeto da licitação pelo período mínimo, sucessivos ou não, de **24 (vinte e quatro) meses**;

7.3.4.1.2 Os atestados apresentados deverão comprovar que a licitante tenha executado ou esteja executando serviços de características técnicas semelhantes ao objeto, relacionadas às seguintes competências:

7.3.4.1.2.1 Monitoramento e gerenciamento de soluções de cibersegurança;

7.3.4.1.2.2 Detecção e resposta de incidentes de cibersegurança em regime contínuo e ininterrupto (24×7x365), envolvendo ao menos ações relacionadas a Inteligência de ameaças (threat intelligence), caçada de ameaças (threat hunting) e gerenciamento de crises cibernéticas;

7.3.4.1.2.3 Gestão de vulnerabilidades de cibersegurança;

7.3.4.1.2.4 Fornecimento e implementação de soluções de cibersegurança (não havendo necessidade de correspondência exata ao rol de soluções exigidas, porém devem possuir afinidade com cibersegurança);

7.3.4.1.2.5 Operação com Centro de Operações de Segurança (SOC).

7.3.4.1.3 Será permitido o somatório de atestados para efeito de comprovação de experiência na prestação do serviço, não se exigindo que todos tenham sido prestados a uma única pessoa jurídica de direito público ou privado, desde que a soma atenda o quantitativo mínimo de **1.000 (mil) ativos**, volume que corresponde a aproximadamente 50% do volume atual da CMB;

7.3.4.1.4 Nos atestados deverão estar expressos, no mínimo, as seguintes informações:

7.3.4.1.4.1 Nome e CNPJ do licitante;

7.3.4.1.4.2 Nome e CNPJ do cliente;

7.3.4.1.4.3 Descrição completa do fornecimento/serviço executado que permitam o amplo entendimento dos trabalhos realizados e identifiquem a compatibilidade e semelhança com objeto da licitação;

7.3.4.1.4.4 Período de vigência do contrato;

7.3.4.1.4.5 Nome e e-mail do emissor do atestado;

7.3.4.1.4.6 Data de emissão e assinatura do emissor.

7.3.4.1.5 Não serão considerados os atestados emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente ou que tenham pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da proponente;

7.3.4.1.6 O licitante deverá disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados ofertados na presente licitação, podendo apresentar, dentre outros documentos, cópia do contrato que deu suporte à contratação, Notas Fiscais/Faturas, Notas de Empenho;

7.3.4.1.7 Fica resguardado o direito da **CMB** em efetuar diligências para verificar a veracidade das informações do(s) Atestado(s) apresentado(s).

7.4 Os documentos para habilitação na presente licitação serão apresentados via sistema apenas pela licitante cuja proposta tenha sido aceita na fase de julgamento, após solicitação do Pregoeiro, no prazo mínimo de **2 (duas) horas**, prorrogáveis por igual período.

7.5 Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de mínimo de **2 (duas) horas**, sob pena de inabilitação.

7.6 É facultado ao Pregoeiro prorrogar os prazos estabelecidos nos subitens acima em função da complexidade envolvida na preparação do envio, de ofício ou a partir de

solicitação fundamentada feita pela licitante, antes de findo o prazo, devendo informar a referida providência no *chat* da licitação.

7.7 As certidões que não possuírem prazo de validade somente serão aceitas se as respectivas datas de emissão não excederem a 180 (cento e oitenta) dias de antecedência da data de sua apresentação.

7.7.1 Não se enquadram no subitem anterior documentos tais como o Registro Comercial, Estatuto ou Contrato Social e documentos similares, evidentemente pois sua validade se encerra com a emissão de suas respectivas novas versões.

7.8 Ao(À) Pregoeiro(a) é reservado o direito de solicitar consulta e emitir os documentos que se encontram disponíveis nos respectivos endereços eletrônicos via Internet, no decorrer da licitação, para verificar as condições de habilitação das licitantes, atribuindo-lhes eficácia para fins de habilitação.

7.9 Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

7.9.1 Não serão aceitos documentos com indicação de CNPJ diferentes, salvo aqueles legalmente permitidos.

7.10 Após declarada a licitante vencedora, caso a proposta mais vantajosa tenha sido ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, comprovar a regularização. O prazo poderá ser prorrogado por igual período.

7.10.1 A não-regularização fiscal no prazo previsto no subitem anterior acarretará a decadência do direito de contratação, sem prejuízo das sanções previstas neste Edital, com a reabertura da sessão pública.

7.11 Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro poderá suspender a sessão, informando a data e horário de retorno ou, no caso de impossibilidade, o reinício condicionado a aviso prévio no sistema com, no mínimo, **24 (vinte e quatro) horas** de antecedência.

7.12 Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

7.13 Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

7.13.1 Complementação de informações necessárias para apurar fatos existentes à época da abertura do certame e/ou que comprovem condição atendida pela licitante através de documentos não apresentados por equívoco ou falha na juntada, adotando-se o princípio do formalismo moderado;

7.13.2 Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

7.14 Na análise dos documentos de habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante despacho fundamentado registrado e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.15 Constatado o atendimento às exigências de habilitação fixadas no Edital, a licitante será declarada vencedora do certame.

7.16 Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

8. DOS RECURSOS

8.1 Qualquer licitante poderá, no prazo de **15 (quinze) minutos**, registrar sua intenção de recorrer em campo próprio do sistema, ao final da fase de julgamento das propostas, após à habilitação ou inabilitação de licitação e em decorrência de anulação ou revogação da licitação.

8.2 As razões de recurso deverão ser apresentadas em momento único, em campo próprio do sistema, no prazo de **5 (cinco) dias úteis**, contados da data de intimação ou de lavratura da Ata da Sessão Pública.

8.3 As demais licitantes ficarão intimadas para, caso desejarem, apresentar suas contrarrazões, no prazo de **5 (cinco) dias úteis**, contado da data de divulgação da interposição do recurso.

8.4 Os recursos e contrarrazões deverão ser encaminhados exclusivamente em campo próprio do sistema.

8.5 O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de **3 (três) dias úteis**, ou, nesse mesmo prazo, encaminhar o recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de **10 (dez) dias úteis**, contado do recebimento dos autos.

8.6 Quanto o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação da licitante a intenção de recorrer deverá ser manifestada imediatamente, no prazo do subitem 8.1, sob pena de preclusão.

8.7 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.8 O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.8.1 A sessão pública poderá ser reaberta nas hipóteses de provimento de recurso que leve à anulação de atos anteriores, situação em que serão repetidos os atos anulados e os que dele dependam.

8.9 A vista dos autos do processo desta licitação poderá ser solicitada ao pregoeiro, pelo e-mail licitacoes@cmb.gov.br.

9. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

9.1 Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade competente definida pelo Regulamento de Licitações e Contratos da CMB para adjudicar o objeto e homologar o procedimento, observado o disposto no art. 71 da Lei nº 14.133, de 2021.

10. DO CONTRATO

10.1 Homologado o resultado da licitação, terá o adjudicatário o prazo de 10 (dez) dias úteis, contados a partir da data de sua convocação por e-mail, para assinar o Instrumento Contratual de forma digital, preferencialmente com certificação ICP-Brasil, podendo ser utilizado o portal de assinatura digital do Instituto Nacional de Tecnologia da Informação – ITI (https://assinador.iti.br/assinatura/indez.xhtml), sob

pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

10.1.1 O prazo previsto no subitem acima poderá ser prorrogado uma única vez, por igual período, por solicitação justificada do fornecedor, e aceita pela CMB.

10.2 O Instrumento Contratual deverá ser assinado por representante legal, diretor ou sócio da empresa, com apresentação, conforme o caso e, respectivamente, de procuração ou contrato social, acompanhados de cédula de identidade.

10.3 Como condição de contratação deverão ser apresentadas todas e quaisquer licenças, alvarás e autorizações pertinentes à atividade objeto, bem como, quando for o caso, o respectivo registro do profissional responsável no órgão de classe competente.

10.3.1 Constitui-se condição de contratação a ausência de registros perante o Cadastro Informativo de Créditos não quitados do setor público federal.

10.4 Na assinatura do Instrumento Contratual, será exigida a comprovação das condições de habilitação consignadas no Edital e/ou Termo de Referência/Especificação dos Serviços, que deverão ser mantidas pelo licitante durante a vigência do contrato.

10.5 Na hipótese de a Adjudicatária não comprovar a manutenção das condições de habilitação consignadas no edital ou se recusar a assinar o instrumento de contratação, a CMB, sem prejuízo da aplicação das sanções previstas neste Edital e das demais cominações legais cabíveis, poderá convocar outro licitante, respeitada a ordem de classificação, para, após analisada a proposta, feita a negociação e comprovado o atendimento dos requisitos para habilitação e eventuais documentos complementares, assinar o instrumento de contratação.

11. DA GARANTIA DE EXECUÇÃO

11.1 As regras acerca da garantia de execução do instrumento de contratação são as estabelecidas no Instrumento Contratual, que segue como parte integrante deste Edital, no ANEXO IV.

12. DO REAJUSTE

12.1 Os critérios de reajuste são os estabelecidos no instrumento de contratação, que segue como parte integrante deste Edital, no Anexo IV.

13. DA ENTREGA E DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

13.1 Os critérios de recebimento e aceitação do objeto e de fiscalização são aqueles previstos no Termo de Referência – ANEXO I e no Instrumento Contratual – ANEXO IV.

14. DAS OBRIGAÇÕES DA CMB

14.1 As obrigações da CMB são as estabelecidas no Instrumento Contratual, que segue como parte integrante deste Edital, no ANEXO IV.

15. OBRIGAÇÕES DA CONTRATADA

15.1 As obrigações da CONTRATADA são as estabelecidas no Instrumento Contratual, que segue como parte integrante deste Edital, no ANEXO IV.

16. DO PAGAMENTO

16.1 As regras acerca do pagamento são aquelas previstas no Termo de Referência – ANEXO I e no Instrumento Contratual – ANEXO IV.

17. DAS SANÇÕES ADMINISTRATIVAS

17.1 Comete infração administrativa, nos termos da Lei nº 13.303, de 2016, a licitante/adjudicatária que, com dolo ou culpa:

17.1.1 deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a Pregoeiro/a durante o certame;

17.1.2 Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

17.1.2.1 não enviar a proposta adequada ao último lance ofertado ou após a negociação;

17.1.2.2 recusar-se a enviar o detalhamento da proposta quando exigível;

17.1.2.3 pedir para ser desclassificado quando encerrada a etapa competitiva; ou

17.1.2.4 deixar de apresentar amostra;

17.1.2.5 apresentar proposta ou amostra em desacordo com as especificações do edital;

17.1.3 não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

17.1.3.1 recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

17.1.4 apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

17.1.5 fraudar a licitação;

17.1.6 comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

17.1.6.1 agir em conluio ou em desconformidade com a lei;

17.1.6.2 induzir deliberadamente a erro no julgamento;

17.1.6.3 apresentar amostra falsificada ou deteriorada;

17.1.7 praticar atos ilícitos com vistas a frustrar os objetivos da licitação praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

17.2 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

17.3 O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, nos termos da Lei nº 13.303, de 2016, às seguintes sanções:

17.3.1 Advertência;

17.3.2 Multa de até 10% (dez por cento) sobre o valor da proposta;

17.3.3 Suspensão temporária de participação em licitação e impedimento de contratar com a CMB, por prazo não superior a 2 (dois) anos;

17.4 As penalidades de advertência e suspensão temporária de participação em licitação e de contratar com a CMB poderão ser aplicadas juntamente com a penalidade de multa.

17.5 As sanções de caráter patrimonial observarão o valor limite da proposta.

17.6 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à licitante/adjudicatária.

17.7 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à CMB, observado o princípio da proporcionalidade.

17.8 Sem prejuízo da aplicação de penalidades, o contratado é responsável pelos danos causados à Administração ou a terceiros na forma disposta no artigo 76 da Lei 13.303, de 2016, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo órgão interessado.

17.9 As penalidades serão obrigatoriamente registradas no SICAF.

17.10 As sanções por atos praticados no decorrer da contratação estão previstas no instrumento de contratação.

17.11 As multas previstas, quando aplicadas, deverão ser recolhidas na Seção de Administração de Tesouraria - SETES da CMB no prazo de até 10 (dez) dias úteis, contados do recebimento da notificação por correio ou outro meio qualquer, que ateste o recebimento.

17.11.1 Caso não haja recolhimento no prazo indicado no subitem acima e o valor da multa for superior ao valor da garantia prestada, quando houver, além da perda desta, responderá a licitante pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela CMB ou, ainda, quando for o caso, cobrada judicialmente nos termos dos artigos 82, §§ 2° e 3°, e 83, § 1°, da Lei 13.303, de 2016.

17.12 Quando interposto, o recurso deverá ser entregue assinado digitalmente pelo representante da contratada ou seu procurador devidamente constituído, em até **10 (dez) dias úteis**, contrarrecibo, ao Departamento de Contratações (DEGEC), que o receberá através da Seção de Emissão de Contratos (SEECT) pelo e-mail seect@cmb.gov.br.

18. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

18.1 Até **05 (cinco) dias úteis** antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

18.2 A impugnação poderá ser realizada por forma eletrônica, pelo e-mail rsimiao@cmb.gov.br c/c licitações@cmb.gov.br, devendo ser informado no campo "assunto" a modalidade e o número desta licitação (Pregão Eletrônico CMB nº xxx/20## – [OBJETO] A/C Pregoeira Rosana Simião).

18.3 Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

18.4 Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até **03 (três) dias úteis** anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

18.5 Caberá ao Pregoeiro decidir sobre a impugnação, bem como responder aos pedidos de esclarecimentos no prazo de **03 (três) dias úteis**, contado da data de recebimento do pedido.

18.6 As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

18.6.1 A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

18.7 As respostas às impugnações e os esclarecimentos prestados pelo Pregoeiro serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado.

19. DAS DISPOSIÇÕES GERAIS

19.1 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário pelo Pregoeiro.

19.2 Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

19.3 É facultado ao Pregoeiro, em qualquer fase do pregão, promover diligências destinadas a esclarecer, sanear ou complementar a instrução do processo desta licitação, constituindo meio legal de prova os documentos obtidos.

19.4 No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

19.5 A qualquer tempo poderá a CMB negociar com a Licitante, com a finalidade de obtenção de proposta mais vantajosa.

19.6 As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados e à luz do princípio do formalismo moderado, desde que não comprometam o interesse da CMB, o princípio da isonomia, a finalidade e a segurança da contratação.

19.7 A aplicação dos normativos expedidos pela Secretaria de Gestão do Ministério da Gestão e Inovação em Serviços Públicos limitar-se-á aos aspectos operacionais inerentes à parametrização do Sistema Eletrônico Compras do Governo Federal, prevalecendo os normativos regulamentares da CMB, inclusive este Edital, no que toca à disciplina da fase preparatória da contratação, atuação do Pregoeiro, prazos e procedimentos de envio da documentação pelas licitantes, diligências e saneamento de falhas, aplicação de sanções e procedimentos posteriores à homologação.

19.8 As limitações operacionais porventura existentes Sistema Eletrônico Compras do Governo Federal decorrentes de imposições normativas no âmbito do Sistema de Serviços Gerais – SISG de que trata o Decreto nº 1.094/1994, não vinculam a CMB, podendo ser adotadas medidas para sua superação, prevalecendo, nesses casos, a instrução constante do processo administrativo correspondente ao certame.

19.9 Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a CMB não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

19.10 Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na CMB.

19.11 O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

19.12 É vedado à CMB, à licitante e a seus empregados, prepostos e gestores: a) frustrar, fraudar mediante qualquer expediente o caráter competitivo do procedimento licitatório público; ou b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público; nos termos da Lei nº 12.846/2013 e suas alterações, do Decreto nº 8420/2015, e suas alterações, ou de quaisquer outras leis ou regulamentos aplicáveis (“Leis Anticorrupção”), ainda que não relacionadas com o presente Edital.

19.13 Reclamações e denúncias relativas a irregularidades ou ao descumprimento pela CMB de suas normas internas ou da legislação vigente durante a condução deste procedimento licitatório poderão ser apresentadas à Ouvidoria da CMB, por meio eletrônico (no endereço eletrônico www.casadamoeda.gov.br ou por meio de correio eletrônico ouvidoria@cmb.gov.br), por meio postal endereçado à Ouvidoria CMB na Rua René Bittencourt n° 371, Distrito Industrial de Santa Cruz, Rio de Janeiro/RJ ou pelo telefone (21) 2184-2969.

19.14 As licitantes poderão marcar, previamente, com a Seção de Infraestrutura - SEINF, localizada na CMB, dia e horário, a fim de procederem, até 05 (cinco) dias consecutivos da data marcada para a abertura dos trabalhos da licitação, às vistorias, exames e medições dos locais onde serão realizados os serviços, não podendo o interessado, posteriormente, arguir omissões, enganos e erros na elaboração da proposta. Qualquer falha na elaboração de seus custos não isentará a licitante da responsabilidade da avaliação correta do orçamento e planejamento dos serviços, arcando com eventuais prejuízos.

19.14.1 Por imposição dos procedimentos e normas de segurança para liberação do acesso à CMB, as visitas só poderão ser realizadas se marcadas com 48 (quarenta e oito) horas de antecedência, pelo e-mail seinf.segredes@cmb.gov.br .

19.14.2 Quando da vistoria, as licitantes deverão inteirar-se das condições e do grau de dificuldade dos trabalhos, não se admitindo, posteriormente, qualquer alegação de desconhecimento dos mesmos.

19.15 Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

19.16 O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.gov.br/compras/pt-br/ e www.casadamoeda.gov.br.

19.17 Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

19.17.1 ANEXO I – Termo de Referência

19.17.2 ANEXO II – Cláusulas e condições para elaboração da proposta

19.17.3 ANEXO III – Minuta de procuração

19.17.4 ANEXO IV – Instrumento Contratual - Minuta do Contrato

Rio de Janeiro, RJ, 18 de novembro de 2026.

Assinatura da Autoridade Competente

Edital publicado pela Pregoeira Rosana Simião.

ANEXO I

TERMO DE REFERÊNCIA

(Processo Administrativo n.º 18750.002778/2025-01)

1. DO OBJETO

1.1. Contratação de empresa especializada para prestação de **Serviço Gerenciado de Segurança (Managed Security Services - MSS) com fornecimento de soluções tecnológicas de cibersegurança**, conforme condições, quantidades e exigências estabelecidas neste instrumento;

1.2. O objeto será adjudicado pelo **Menor Preço Global**, em **Regime de Empreitada por Preço Global**, conforme tabela abaixo:

Item	Descrição/Especificação	Qnt.	Unidade de Medida	Código CMB	Nº Solicitação de Compra	CatMat similar ou equivalente
1	Serviço Gerenciado de Segurança (Managed Security Services - MSS) com Fornecimento de Soluções Tecnológicas de Cibersegurança	36	meses	S10884	114911	27014

1.3. O objeto consistirá na prestação de Serviço Gerenciado de Segurança (Managed Security Services - MSS), abrangendo as atividades de gestão de soluções cibernéticas, gestão de incidentes cibernéticos e gestão de vulnerabilidades cibernéticas, bem como a implementação, configuração e operação de soluções tecnológicas de cibersegurança de última geração, visando auxiliar na prestação deste serviço;

1.4. Todo o objeto deve ser comercializado na forma de serviço, não havendo aquisição direta de bens nesta contratação;

1.5. O objeto enquadra-se na categoria de bens comuns, por possuir padrões de desempenho e qualidade que possam ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado;

1.6. O objeto da presente licitação trata-se de serviço continuado, sem necessidade de dedicação exclusiva de mão-de-obra;

1.7. O detalhamento integral do objeto a ser contratado encontra-se descrito na "**Especificação Técnica" (APENSO A)** deste Termo de Referência, a qual

apresenta todas as características, requisitos e condições necessárias para a plena compreensão da solução pretendida.

2. DA JUSTIFICATIVA DA CONTRATAÇÃO

A Casa da Moeda do Brasil (CMB), por meio de seu Departamento de TI Corporativo e Comunicação (DETIC), é responsável por assegurar a confidencialidade, integridade e a disponibilidade de todo o seu parque tecnológico, primando sempre a qualidade e a confiabilidade dos serviços prestados pela organização. Em consonância com os objetivos estabelecidos em seu Plano Estratégico Institucional (PEI) e no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), a CMB vem realizando investimentos para modernizar e aprimorar sua infraestrutura tecnológica, de forma a consolidar a Tecnologia da Informação e Comunicação (TIC) como um importante instrumento facilitador dessas estratégias. Tais investimentos buscam principalmente manter a empresa competitiva e alinhada às melhores práticas do mercado, visando otimizar seus processos, aumentar a sua eficiência operacional e oferecer uma experiência cada vez mais segura, integrada e satisfatória aos seus funcionários, clientes, parceiros e sociedade.

Embora a modernização tecnológica seja essencial para o crescimento e a inovação contínua da CMB, é imprescindível que essa trajetória seja conduzida com um compromisso firme com a Segurança da Informação (SI), dado que as ameaças cibernéticas representam riscos cada vez mais sofisticados e prejudiciais capazes de causar danos que vão desde a interrupção das operações, até a exposição de dados sensíveis, o que pode resultar em prejuízos financeiros e comprometimento da reputação da organização. Nesse contexto, esta contratação tem o principal objetivo de fortalecer a postura de segurança cibernética da CMB, promovendo melhorias significativas que visam aumentar a visibilidade de riscos relevantes que podem impactar os negócios, além de ampliar a sua capacidade de resposta a incidentes, garantindo uma maior resiliência e proteção dos seus ativos críticos.

Relatórios especializados em cibersegurança mundialmente respeitados, produzidos anualmente por empresas de destaque no setor, fornecem um panorama abrangente sobre o cenário atual e futuro das ameaças, destacando o tema cibersegurança como uma das preocupações centrais das empresas em todo o mundo. Um ponto comum entre os relatórios é a crescente sofisticação dos ataques, consolidando um novo patamar na evolução das ameaças, impulsionadas principalmente pelo advento da inteligência artificial (IA), o que vem forçando as empresas a reavaliem suas estratégias de segurança. Na América Latina, desde 2013 o Brasil já é considerado como o principal alvo de ataques cibernéticos, sendo um dos países mais visados pelos criminosos digitais em todo o mundo.

No âmbito do governo federal, observa-se um crescente comprometimento com o fortalecimento da segurança da informação e cibersegurança, buscando proteger dados públicos, assegurar a soberania digital e preparar o país para os desafios do mundo conectado. Nesse cenário, destacam-se a Política Nacional de Segurança da Informação (PNSI – Decreto nº 9.637/2018), de caráter abrangente, voltada à proteção da informação em meios digitais, físicos e virtuais, e a Política Nacional de Cibersegurança (PNCiber – Decreto nº 11.856/2023), mais recente e especializada, direcionada ao fortalecimento da resiliência cibernética. Juntas, essas políticas formam os pilares estratégicos do Brasil para enfrentar as ameaças digitais contemporâneas. Corroborando essas iniciativas, dados recentes providos pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR-Gov), mostram que o ano de 2024 contabilizou cerca 9,8 mil incidentes em instituições públicas, quase o dobro se comparado ao ano anterior. Em 2025, até o mês de setembro, já foram contabilizados cerca de 7,3 mil incidentes.

Diante da crescente dependência tecnológica em suas operações, a CMB encontra-se cada vez mais exposta a ameaças cibernéticas, o que torna a cibersegurança um eixo central na definição de suas estratégias de negócio. Proteger-se nesse cenário exige uma abordagem robusta, proativa e integrada, baseada na adoção de medidas automatizadas capazes de detectar e neutralizar ataques cada vez mais sofisticados e direcionados. Nesse contexto, o uso de tecnologias avançadas apoiadas em inteligência artificial (IA) torna-se indispensável, pois potencializa a identificação de ameaças, acelera a resposta a incidentes e permite adaptação contínua frente a novas vulnerabilidades, assegurando a proteção dos dados da CMB e a continuidade de suas operações.

Embora a CMB já adote diversas políticas, procedimentos e tecnologias voltadas à cibersegurança, o avanço contínuo e a crescente sofisticação das ameaças digitais tornam a contratação de serviços e soluções especializadas não apenas uma escolha, mas uma necessidade estratégica. Garantir a continuidade dos negócios, proteger a reputação institucional e assegurar a conformidade regulatória dependem diretamente da capacidade técnica e operacional de atuar de forma proativa na prevenção e contenção de riscos cibernéticos. Nesse sentido, o investimento em cibersegurança reafirma o compromisso da CMB com a excelência operacional e a proteção da informação, além de alinhar seus processos de modernização e inovação tecnológica às melhores práticas do mercado, promovendo um crescimento sustentável, seguro e confiável.

3. DO PARCELAMENTO DA CONTRATAÇÃO

3.1. Em função dos aspectos técnicos que envolvem a contratação e considerando o grau de interação das atividades a serem desenvolvidas, a natureza específica, o caráter contínuo, aliada a alta criticidade e complexidade do ambiente de TI da CMB, optou-se por uma contratação unificada, uma vez que a contratação individualizada do objeto não atenderia plenamente as necessidades e objetivos almejados pela CMB;

3.2. Optar pela contratação de um único prestador de serviços oferece a vantagem estratégica da gestão centralizada, simplificando a supervisão e a priorização dos esforços de proteção digital da organização. Isso não apenas otimiza a identificação de riscos e a resposta a incidentes, mas também garante a implementação de políticas de segurança de forma mais coesa e eficiente, permitindo que a equipe interna se concentre em tarefas mais estratégicas para o negócio;

3.3. Entende-se que a gestão das soluções tecnológicas e das atividades envolvidas devem ocorrer de forma altamente integrada e coordenada, sendo crucial uma visão totalmente unificada do ambiente para alcançar uma resposta proativa a qualquer ameaça ou incidente de segurança que possa comprometer a CMB, minimizando o seu impacto potencial;

3.4. A concentração do objeto sobre um único prestador de serviços potencializa uma visão holística da segurança, facilitando a integração das descobertas e medidas de mitigação em uma estratégia de segurança unificada. A gestão fragmentada pode levar a falta de uma sinergia natural, lacunas na comunicação e do entendimento claro das suas responsabilidades, colocando em risco a estratégia de cibersegurança da CMB, no qual a agilidade na descoberta e tratamento de incidentes e ameaças é vital para a eficiência da proteção dos dados e ativos organizacionais;

3.5. A presença de múltiplos prestadores de serviços dificulta a definição de responsabilidades em casos de falhas de segurança, favorecendo a transferência de atribuições e atrasando tanto a resolução de problemas quanto a adoção de melhorias necessárias. A ausência de uma coordenação centralizada amplia o risco de lacunas na proteção, uma vez que cada prestador pode presumir que outro esteja cobrindo determinado aspecto da segurança, ocasionando áreas potencialmente desprotegidas e vulneráveis a ataques;

3.6. A utilização de diferentes prestadores de serviços pode implicar no emprego de tecnologias e metodologias pouco compatíveis entre si, gerando conflitos nas

soluções implementadas e reduzindo a eficácia das defesas. Esse cenário torna a gestão do ambiente de segurança mais complexa, ao mesmo tempo em que a fragmentação administrativa pode ocasionar redundâncias, sobreposições de atividades e elevação dos custos operacionais. Em contrapartida, a centralização em um único prestador favorece uma gestão mais ágil, integrada e menos suscetível a falhas, elevando a eficiência operacional, em vez de lidar com problemas decorrentes da falta de integração entre múltiplos prestadores de serviços;

3.7. A atuação de múltiplos prestadores de serviços dificulta a gestão do conhecimento sobre o ambiente de segurança da CMB, impedindo a consolidação de uma base unificada que sustente a melhoria contínua das defesas. Ao concentrar os serviços em um único prestador, a CMB reduz esse risco, promovendo uma estratégia de segurança mais robusta e eficiente, com comunicação clara, responsabilidades bem definidas e uma visão integrada das necessidades de proteção;

3.8. Sob o aspecto de custos, a contratação de um único prestador de serviços pode gerar economias de escala, uma vez que uma única empresa consegue oferecer pacotes integrados a preços mais competitivos. A centralização permite otimizar recursos, reduzir redundâncias e obter condições financeiras mais vantajosas;

3.9. Do ponto de vista da segurança, a centralização dos serviços em um único prestador de serviços reduz o risco de comprometimento da confidencialidade de informações sensíveis, uma vez que a atuação de múltiplos prestadores eleva a probabilidade de exposição de dados. Um único prestador possibilita a implementação de uma política de segurança unificada, garantindo uma uniformidade dos processos, além de restringir o acesso aos dados sensíveis a um número mais reduzido de pessoas;

3.10. O agrupamento não prejudicará a competitividade do certame, considerando a ampla disponibilidade no mercado de prestadores de serviços qualificados e capacitados a executar integralmente o objeto. Esses prestadores poderão compor suas soluções utilizando diferentes fabricantes de tecnologias, permitindo, assim, a apresentação de propostas diversificadas e competitivas.

4. DO CONTROLE DA EXECUÇÃO

4.1. Em cumprimento ao art. 40, VII c/c 69 da Lei nº 13.303/16, o Superintendente do Departamento de TI Corporativo e Comunicação (DETIC) da CMB designará

representante para acompanhar e fiscalizar a entrega do objeto, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados;

4.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da CMB ou de seus agentes e prepostos, em conformidade com o art. 76 da Lei nº 13.303/16.

4.3. O fiscal do instrumento contratual anotará em registro próprio todas as ocorrências relacionadas com a execução do instrumento contratual, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

5. DA DINÂMICA CONTRATUAL

5.1. A tabela a seguir apresenta os principais entregáveis previstos na execução contratual. É imprescindível que a CONTRATADA observe e cumpra rigorosamente todos os prazos estabelecidos para cada etapa;

CRONOGRAMA DE ENTREGÁVEIS			
ETAPA	**DESCRIÇÃO**	**PRAZO**	**RESPONSÁVEL**
1	Convocação para assinatura do contrato	---	CMB
2	Entrega dos documentos comprobatórios de credenciamento/parceria/autorização do fabricante	Até 5 (cinco) dias úteis após a etapa 1	CONTRATADA
3	Entrega dos documentos comprobatórios qualificação da equipe técnica	Até 5 (cinco) dias úteis após a etapa 1	CONTRATADA
4	Assinatura do contrato	Até 5 (cinco) dias úteis após a etapa 2 e 3	CONTRATADA
5	Indicação de preposto e seu substituto	Até 5 (cinco) dias úteis após a conclusão da etapa 4	CONTRATADA

6	Assinatura do Acordo de Confidencialidade	Até 5 (cinco) dias úteis após a conclusão da etapa 4	CONTRATADA
7	Reunião de Alinhamento	Até 5 (cinco) dias úteis após a conclusão da etapa 6	CONTRATADA CMB
8	Implementação da VPN IPSec site-to-site	Até 15 (quinze) dias úteis após a conclusão da etapa 7	CONTRATADA
9	Execução da primeira avaliação de segurança do ambiente da CMB (Assessment de Segurança)	Até 15 (quinze) dias úteis após a conclusão da etapa 7	CONTRATADA
10	Entrega do “Plano de Gerenciamento de Incidentes”	Até 15 (quinze) dias úteis após a conclusão da etapa 7	CONTRATADA
11	Entrega do “Plano de Gerenciamento de Vulnerabilidades”	Até 15 (quinze) dias úteis após a conclusão da etapa 7	CONTRATADA
12	Atesto das Etapas 8 a 11	Até 5 (cinco) dias úteis após a sua conclusão	CMB
13	Reunião Técnica de Alinhamento para entrega das soluções de “Incident Management Platform” e “Network Packet Broker (NPB)”	Até 5 (cinco) dias úteis após a conclusão da etapa 7	CONTRATADA CMB
14	Entrega do “Plano de Implementação das Soluções” de “Incident Management Platform” e “Network Packet Broker (NPB)”	Até 10 (dez) dias úteis após a conclusão da etapa 13	CONTRATADA
15	Atesto da Etapa 14	Até 5 (cinco) dias úteis após a sua conclusão	CMB
16	Entrega das soluções de “Incident Management Platform” e “Network Packet Broker (NPB)”	Até 40 (quarenta) dias úteis após a conclusão da etapa 15	CONTRATADA

17	Entrega do “Relatório de Conclusão da Implementação (as-built)” das soluções de “Incident Management Platform” e “Network Packet Broker (NPB)”	Até 40 (quarenta) dias úteis após a conclusão da etapa 15	CONTRATADA
18	Atesto das Etapas 16 e 17	Até 5 (cinco) dias úteis após a sua conclusão	CMB
19	Reunião Técnica de Alinhamento para entrega das soluções de “Vulnerability Management Platform”, “Cyber Threat Intelligence Platform (CTI)” e “Breach And Attack Simulation (BAS)”	Até 5 (cinco) dias úteis após a conclusão da etapa 18	CONTRATADA CMB
20	Entrega do “Plano de Implementação das Soluções” de “Vulnerability Management Platform”, “Cyber Threat Intelligence Platform (CTI)” e “Breach And Attack Simulation (BAS)”	Até 10 (dez) dias úteis após a conclusão da etapa 19	CONTRATADA
21	Atesto da Etapa 20	Até 5 (cinco) dias úteis após a sua conclusão	CMB
22	Entrega das soluções de “Vulnerability Management Platform”, “Cyber Threat Intelligence Platform (CTI)” e “Breach And Attack Simulation (BAS)”	Até 10 (dez) dias úteis após a conclusão da etapa 21	CONTRATADA
23	Entrega do “Relatório de Conclusão da Implementação (as-built)” das soluções de “Vulnerability Management Platform”, “Cyber Threat Intelligence Platform (CTI)” e “Breach And Attack Simulation (BAS)”	Até 10 (dez) dias úteis após a conclusão da etapa 21	CONTRATADA
24	Atesto das Etapas 22 e 23	Até 5 (cinco) dias úteis após a sua conclusão	CMB
25	Reunião Técnica de Alinhamento para entrega das soluções de “Web Application Security Platform”, “Security Service Edge (SSE)” e “Unified Identity Security Platform”	Até 5 (cinco) dias úteis após a conclusão da etapa 24	CONTRATADA CMB
26	Entrega do “Plano de Implementação das Soluções” de “Web Application Security Platform”, “Security Service Edge (SSE)” e “Unified Identity Security Platform”	Até 10 (dez) dias úteis após a conclusão da etapa 25	CONTRATADA
27	Atesto da Etapa 26	Até 5 (cinco) dias úteis após a sua conclusão	CMB

28	Entrega das soluções de “Web Application Security Platform”, “Security Service Edge (SSE)” e “Unified Identity Security Platform”	Até 15 (quinze) dias úteis após a conclusão da etapa 27	CONTRATADA
29	Entrega do “Relatório de Conclusão da Implementação (as-built)” das soluções de “Web Application Security Platform”, “Security Service Edge (SSE)” e “Unified Identity Security Platform”	Até 15 (quinze) dias úteis após a conclusão da etapa 27	CONTRATADA
30	Atesto das Etapas 28 e 29	Até 5 (cinco) dias úteis após a sua conclusão	CMB
31	Início da gestão das soluções listadas em “Soluções Internas” (APENSO H) deste Termo de Referência	Até 10 (dez) dias úteis após a conclusão da etapa 30	CONTRATADA

5.2. Após a homologação do licitante vencedor no certame, será obrigatória, como **condição para a formalização/assinatura do Contrato**, a comprovação de credenciamento/parceria/autorização junto aos fabricantes das soluções tecnológica ofertadas, devendo estar devidamente habilitada e autorizada a comercializar seus respectivos produtos e licenças;

5.2.1. Este requisito busca garantir a contratação adequada de produtos e licenças, mitigando os riscos associados ao fornecimento de licenças não oficiais ou com suporte inadequado por parte do fabricante. Visa também confirmar que a CONTRATADA possui as competências e habilidades necessárias para comercializar tal produto, garantindo que a CMB tenha acesso a atualizações regulares e recursos de segurança robustos, cruciais para a operação contínua e segura dos sistemas;

5.2.2. A comprovação deverá ocorrer, exclusivamente, por meio de documento oficial emitido diretamente pelo fabricante da solução, em data compatível com o processo licitatório;

5.2.3. O documento de comprovação apresentado pela CONTRATADA estará sujeito à análise da CMB, que reserva-se o direito de realizar validação direta junto ao fabricante para confirmar sua autenticidade.

5.3. Após a homologação da licitante vencedora no certame, será obrigatória, como **condição para a formalização/assinatura do Contrato**, a comprovação do atendimento aos requisitos mínimos de qualificação da equipe técnica, conforme estabelecido na **“Especificação Técnica” (APENSO A)** deste Termo de Referência, especialmente na seção “Quanto à Qualificação da Equipe”;

5.3.1. Este requisito busca assegurar que o serviço seja executado com o nível adequado de capacidade técnica, eficiência e qualidade, em consonância com os resultados esperados pela CMB. Considerando que o objeto da contratação demanda conhecimentos especializados e atuação técnica qualificada, a verificação prévia da aptidão da equipe reduz riscos operacionais, mitiga a possibilidade de falhas na execução e contribui para o cumprimento dos níveis de serviço estabelecidos;

5.3.2. A comprovação deverá ocorrer mediante a apresentação de documentação idônea que evidencie o atendimento integral aos requisitos mínimos de qualificação exigidos, tais como certificados, diplomas, atestados de capacidade técnica, vínculos profissionais e demais documentos pertinentes;

5.3.3. A documentação apresentada será analisada pela CMB, que poderá, a seu critério, solicitar esclarecimentos ou complementações, a fim de verificar a aderência aos requisitos estabelecidos.

5.4. A CONTRATADA deverá indicar formalmente um preposto (e seu substituto) idôneo com poderes de decisão para representá-la junto à CMB;

5.4.1. Deverão ser informados ao menos os seguintes dados do preposto e seu substituto: nome completo, cargo, telefone e endereço de e-mail;

5.4.2. O preposto será responsável, entre outros atividades, por acompanhar a execução do contrato e atuar como interlocutor principal junto à CMB, incumbido de receber, diligenciar, encaminhar e responder as principais questões referentes ao andamento contratual;

5.4.3. A CONTRATADA deverá informar imediatamente sempre que houver mudança do seu preposto ou substituto, devendo encaminhar para a CMB as informações pertinentes do novo representante.

5.5. A CONTRATADA deverá realizar **“Reunião de Alinhamento”** com a CMB, que será destinada para assegurar que as partes compreendam claramente os objetivos, expectativas e requisitos relacionados à contratação, visando garantir um início de trabalho harmonioso, e maximizar a eficácia da entrega do objeto da contratação. Nesta reunião, deverão ser abordados minimamente os seguintes pontos:

I. Apresentação geral do Centro de Operações de Segurança (Security Operation Center - SOC) destacando sua infraestrutura, os principais processos operacionais e as ferramentas que sustentam suas principais

atividades, bem como os mecanismos internos de colaboração entre as equipes, que garantem agilidade e eficiência na prestação do serviço;

II. Apresentação geral (overview) de todas as soluções tecnológicas a serem fornecidas, destacando suas principais funcionalidades;

III. Apresentação da qualificação e a experiência do(s) profissional(is) que atuará(ão) como coordenador(es) do projeto de implementação das soluções, destacando competências técnicas, trajetória profissional e atuação em projetos similares;

IV. Apresentação de um plano preliminar do projeto que compreenda as necessidades gerais da CMB, em conformidade com os requisitos do Termo de Referência, incluindo ao menos as principais metas a serem alcançadas e os mecanismos propostos para avaliação, monitoramento e controle das atividades;

V. Levantamento das informações necessárias para elaboração do **"Plano de Gerenciamento de Incidentes"** e do **"Plano de Gerenciamento de Vulnerabilidades"**, nos moldes deste Termod e Referência;

VI. Levantamento das informações necessárias para estabelecimento do túnel VPN IPSec entre a CMB e os SOC's redundantes da CONTRATADA;

VII. Levantamento das informações necessárias para primeira execução da avaliação da segurança do ambiente da CMB (Assessment de Segurança), com o objetivo identificar lacunas e oportunidades de melhoria (Gap Analysis);

VIII. Definição dos canais de comunicação que deverão ser utilizados para viabilizar a comunicação direta entre as partes, visando facilitar e agilizar ajustes e melhorias contínuas na prestação do serviço.

5.6. A CONTRATADA deverá desenvolver, em colaboração com a CMB, um **"Plano de Gerenciamento de Incidentes"**, visando documentar todas as informações necessárias para assegurar uma resposta eficaz e coordenada aos eventos de cibersegurança. O plano deverá estabelecer, no mínimo, as seguintes informações:

I. **Plano de Comunicação de Incidentes:** Detalhar quem deve ser contatado (incluindo contatos internos e externos), como deve ser contatado (canais de comunicação primários e alternativos) e quando deve ser contatado (gatilhos e prazos). Deve-se incluir ainda procedimentos claros para lidar com falhas de comunicação e escalonamento;

II. **Identificação de Equipes e Responsabilidades:** Designar claramente as equipes e indivíduos responsáveis por cada fase do gerenciamento de incidentes, incluindo detecção, análise, contenção, erradicação, recuperação e análise pós-incidente;

III. **Armazenamento de Evidências:** Estabelecer métodos e locais seguros para a coleta, preservação e armazenamento de todas as evidências e informações relacionadas aos incidentes. Isso inclui logs, imagens, artefatos de malware e qualquer outro dado relevante para a investigação e, se necessário, para processos legais;

IV. **Monitoramento de Ativos:** Definir todos os tipos de ativos que serão monitorados e os recursos tecnológicos a serem utilizados para identificação e análise de incidentes;

V. **Identificação de Alvos Críticos:** Definir os principais alvos críticos a serem monitorados proativamente, englobando ativos essenciais, setores estratégicos, regiões geográficas específicas, marcas da CMB e usuários com acessos privilegiados ou sensíveis;

VI. **Levantamento de Recursos Necessários:** Identificar todos os recursos necessários para a implementação e execução eficaz dos processos de gerenciamento de incidentes;

VII. **Definição de Tipos de Alertas:** Estabelecer os diferentes tipos de alertas iniciais a serem ativados, especificando as condições para o acionamento de notificações ou encadeamento de ações automáticas de resposta (Ex: bloqueio de IP, isolamento do host, entre outros);

VIII. **Definição de Relatórios:** Definir os tipos de relatórios de segurança a serem adotados periodicamente para padronizar o registro de todas as etapas do processo de gerenciamento de incidentes, incluindo relatórios executivos e técnicos;

IX. **Cronograma de Revisão e Melhoria Contínua:** Estabelecer um cronograma claro para a revisão, atualização e melhoria contínua do Plano de Gerenciamento de Incidentes, garantindo sua relevância e eficácia diante de novas ameaças e mudanças na infraestrutura;

X. **Simulações de Ataques:** Definir as técnicas e a periodicidade das simulações de ataque que serão realizadas para testar a eficácia do plano e a prontidão da equipe de resposta a incidentes;

XI. **Monitoramento de Atores de Ameaças:** Especificar as principais fontes de inteligência de ameaças e atores de ameaças (Ex. grupos cibercriminosos, APTs, hacktivistas, entre outros) a serem monitorados inicialmente, com foco naqueles que representam maior risco para a CMB ou seu setor de atuação;

XII. **Procedimento padrão para Incidentes:** Mapear os principais tipos de incidentes de cibersegurança que a CMB pode enfrentar (Ex. malware, DDoS, phishing, ransomware, comprometimento de credenciais, acesso não autorizado, vazamento de dados, engenharia social, ataques a aplicações web, entre outros). Para cada tipo de incidente, devem ser definidos procedimentos operacionais padrão de contenção, que deverão ser desenhados para guiar e facilitar a tomada de decisões pela equipe de resposta, minimizando a propagação e o impacto do incidente;

5.7. A CONTRATADA deverá desenvolver, em colaboração com a CMB, um "**Plano de Gerenciamento de Vulnerabilidades"**, visando consolidar todas as informações cruciais para a identificação, avaliação, tratamento e monitoramento contínuo de vulnerabilidades de cibersegurança. O plano deverá conter, no mínimo, as seguintes informações:

I. **Plano de Comunicação de Vulnerabilidades:** Detalhar quem deve ser contatado, como deve ser contatado (canais de comunicação primários e alternativos) e quando deve ser contatado (gatilhos e prazos). Deve-se incluir ainda procedimentos claros para lidar com falhas de comunicação e escalonamento;

II. **Identificação de Equipes e Responsabilidades:** Designar claramente as equipes e indivíduos responsáveis por cada fase do gerenciamento de vulnerabilidades;

III. **Monitoramento de Ativos:** Definir todos os tipos de ativos que serão monitorados e os recursos tecnológicos a serem utilizados para identificação das vulnerabilidades;

IV. **Identificação de Ativos Críticos:** Definir os principais ativos críticos a serem monitorados, devendo ser atribuída uma nota de risco;

V. **Levantamento de Recursos Necessários:** Identificar todos os recursos necessários para a implementação e execução eficaz dos processos de gerenciamento de vulnerabilidades;

VI. **Definição de Tipos de Alertas:** Estabelecer os diferentes tipos de alertas iniciais a serem ativados, especificando as condições para o acionamento de notificações ou encadeamento de ações automáticas de correção;

VII. **Definição de Relatórios:** Definir os tipos de relatórios de segurança a serem adotados periodicamente para padronizar o registro de todas as etapas do processo de gerenciamento de vulnerabilidades, incluindo relatórios executivos e técnicos;

VIII. **Cronograma de Revisão e Melhoria Contínua:** Estabelecer um cronograma claro para a revisão, atualização e melhoria contínua do Plano de Gerenciamento de Vulnerabilidades, garantindo sua relevância e eficácia diante de novas ameaças e mudanças na infraestrutura;

IX. **Simulações de Ataques:** Definir as técnicas e a periodicidade das simulações de ataque que serão realizadas para testar a eficácia do plano e para teste da eficiência das correções aplicadas;

X. **Periodicidade das Varreduras:** Definição da periodicidade das vulnerabilidades em todo o ambiente da CMB, considerando diferentes tipos de ativos e sua criticidade, o pode incluir varreduras diárias, semanais, mensais ou trimestrais, dependendo do ativo e dos riscos associados.

5.8. A CONTRATADA deverá realizar **"Reunião Técnica de Alinhamento"** com a CMB, a fim de discutir o planejamento da implementação das soluções tecnológicas, o que ocorrerá de forma faseada. Cada fase contemplará um conjunto diferente de soluções a serem implementadas, conforme indicado na tabela de **"Cronograma de Entregáveis"**. Nesta reunião, deverão ser abordados, no mínimo, os seguintes pontos:

I. Apresentação das soluções a serem implementadas, incluindo o detalhamento completo das funcionalidades contratadas, suas aplicações práticas e os benefícios esperados. Recomenda-se o uso de demonstrações ou estudos de caso relevantes para ilustrar o funcionamento e a utilidade das soluções;

II. Apresentação das melhores práticas de mercado e as principais recomendações do fabricante voltadas especificamente para a correta implantação das soluções tecnológicas;

III. Levantamento, em colaboração com a CMB, das configurações que deverão ser aplicadas nas soluções tecnológicas, onde devem ser considerados todos os requisitos mínimos estabelecidos na **"Especificação Técnica" (APENSO A)** deste documento, bem como os requisitos apontados pela CMB nesta reunião;

IV. Levantamento das informações técnicas cruciais e pertinentes para viabilizar a correta prestação do serviço. Caso seja identificado, durante a reunião, a necessidade de informações adicionais que só possam ser obtidas presencialmente, a CONTRATADA poderá agendar uma visita técnica nas instalações da CMB.

5.9. Caberá à CONTRATADA documentar de forma abrangente todas as informações levantadas durante a "**Reunião Técnica de Alinhamento"**, o que será denominado como **"Plano de Implementação das Soluções"**. O documento deverá abordar, no mínimo, os seguintes aspectos:

I. Cronograma granular contendo data, atividades, prazos e os respectivos profissionais responsáveis pela sua execução. A CONTRATADA, visando a correta elaboração do cronograma, deverá assegurar o cumprimento rigoroso dos prazos máximos estabelecidos na tabela "Cronograma de Entregáveis";

II. Diagrama preliminar da topologia que deverá servir de referência para a implementação de cada solução. Este diagrama deve ilustrar a arquitetura proposta e a interconexão dos componentes;

III. Descrição do conjunto de configurações que serão aplicadas nas soluções, conforme estabelecido na "**Reunião de Alinhamento";**

IV. Plano de testes abrangente para validar o funcionamento perfeito das soluções após a sua implantação. Este plano deve incluir a definição dos tipos de testes a serem realizados, os critérios de aceitação e os responsáveis pela aprovação final de cada etapa de teste;

V. Plano de comunicação detalhando como e quando as informações referentes ao progresso da implementação das soluções serão compartilhadas com a CMB, incluindo a frequência das atualizações e os canais de comunicação;

VI. Relatório contendo uma análise dos potenciais impactos da implementação de cada solução na infraestrutura da CMB, bem como as estratégias de mitigação para quaisquer riscos identificados;

VII. Canais de atendimento que deverão ser utilizados pela CMB para abertura e acompanhamento de chamados, bem como para "escalação extraordinária", nos moldes dos requisitos definidos na **"Especificação Técnica" (APENSO A)** deste documento;

VIII. Descrição, de forma clara e objetiva, de todos os pré-requisitos que deverão ser atendidos pela CMB para garantir o sucesso da prestação dos serviços contratados.

5.10. A CONTRATADA deverá elaborar um "**Relatório de Conclusão da Implementação (as-built)"**, destinado para fornecer um registro completo e preciso de como as soluções foram efetivamente implementadas no ambiente da CMB, servindo como uma base sólida para futuras operações, manutenções, auditorias e atualizações. O relatório deverá detalhar, no mínimo, as seguintes informações:

I. **Descrição das Soluções:** Descrição detalhada das principais funcionalidades ativadas, incluindo a versão do software/firmware instalado e as configurações relevantes aplicadas;

II. **Registro de Alterações e Desvios:** Documentar todas as alterações, desvios ou modificações que ocorreram em relação ao planejamento original do projeto. Para cada alteração, incluir uma justificativa técnica, os motivos da decisão, responsável pela aprovação e os possíveis impactos no desempenho, segurança ou futuras expansões;

III. **Configurações Aplicadas:** Detalhamento das configurações implementadas nas soluções, incluindo, por exemplo, endereços IP, políticas de segurança, parâmetros de alta disponibilidade, e demais ajustes técnicos relevantes que garantam o funcionamento adequado e seguro do sistema;

IV. **Resultados dos Testes**: Descrever os resultados obtidos dos testes de validação e verificação efetuados, incluindo critérios de não conformidade identificados e respectivas correções aplicadas;

V. **Recomendações e Considerações Finais**: Apontar boas práticas para operação e manutenção das soluções, riscos identificados, sugestões de melhorias e observações relevantes para garantir a continuidade e evolução do sistema implantado;

5.11. As etapas de "Atesto", conforme indicado na tabela de "Cronograma de Entregáveis", terão a finalidade averiguar a qualidade e conformidade dos

entregáveis realizados pela CONTRATADA com relação às especificações constantes neste Termo de Referência;

5.11.1. Os entregáveis poderão ser rejeitados parcialmente ou totalmente, no qual será emitido LAUDO desfavorável pelo Gestor/Fiscal do Contrato;

5.11.2. Em caso de não conformidade, caberá à CONTRATADA promover, às suas expensas, a correção/refazimento/substituição de todos os elementos apontadas no LAUDO, no prazo máximo de **até 10 (dez) dias úteis**, contados a partir do primeiro dia útil subsequente à data de entrega do LAUDO desfavorável;

5.11.3. A correção/refazimento/substituição dos entregáveis por mais de 2 (duas) vezes poderá ensejar na aplicação de penalidades cabíveis, devendo a CONTRATADA respeitar os prazos máximos definidos;

5.11.4. Todos os entregáveis só serão considerados como "concluídos", estando apta para faturamento, após a emissão do **"Termo de Aceite Definitivo" (APENSO C)** pela CMB, o que ocorrerá apenas após avaliação de que todos os requisitos deste Termo de Referência foram integralmente cumpridos pela CONTRATADA;

5.11.5. A aprovação dos entregáveis não afasta ou diminui a responsabilidade da CONTRATADA por eventuais prejuízos decorrentes da execução incorreta do instrumento contratual que venham a ser identificados posteriormente.

5.12. Os primeiros **90 (noventa) dias corridos,** após a emissão do **"Termo de Aceite Definitivo" (APENSO C),** será considerado como **"Período de Estabilização do Serviço"**, durante o qual os indicadores de qualidade não atingidos, conforme estabelecido em **"Níveis Mínimos de Serviço" (APENSO D)**, ensejarão na aplicação de glosas conforme os seguintes critérios:

I. **Do 1º ao 30º dia:** aplicar-se-á efetivamente apenas 25% (vinte e cinco por cento) do total de eventuais descontos decorrentes do não atingimento dos indicadores de serviço estabelecidos;

II. **Do 31º ao 60º dia:** aplicar-se-á efetivamente apenas 50% (cinquenta por cento) do total de eventuais descontos decorrentes do não atingimento dos indicadores de serviço estabelecidos;

III. **Do 61º ao 90º dia:** aplicar-se-á efetivamente apenas 75% (setenta e cinco por cento) do total de eventuais descontos decorrentes do não atingimento dos indicadores de serviço estabelecidos;

IV. **Após o 90º dia:** aplicar-se-ão efetivamente 100% (cem por cento) do total de eventuais descontos decorrentes do não atingimento dos indicadores de serviço estabelecidos.

5.12.1. Os descontos concedidos durante o "**Período de Estabilização do Serviço"** não serão aplicados em caso de omissão da CONTRATADA em seu dever agir, conforme exigências estabelecidas neste instrumento;

5.12.2. Em caso de prorrogação contratual, não haverá novo **"Período de Estabilização do Serviço"**, ou seja, serão aplicadas integralmente as glosas cabíveis;

5.13. A CONTRATADA, ao final da vigência contratual, deverá ficar à disposição da CMB, pelo período de **até 60 (sessenta) dias corridos**, para fornecer todas as informações necessárias para a correta "transição do serviço" à empresa sucessora;

5.13.1. A CONTRATADA deverá responsabilizar-se pela transição do serviço, de forma que o repasse de informações, conhecimentos e procedimentos aconteçam de forma pacífica, precisa e responsável;

5.13.2. O processo de "transição do serviço" tem o propósito de preparar a nova empresa para assumir integralmente as obrigações advindas com o contrato, sendo baseada em reuniões e repasse de documentos;

5.13.3. Caberá à CONTRATADA atualizar toda a documentação pertinente gerada ao logo da contratação, antes do seu repasse à sucessora;

5.13.4. O processo de "transição do serviço" inicia-se a partir do momento que a empresa sucessora assumir a responsabilidade pelos serviços prestados por meio da formalização da assinatura do contrato;

5.13.5. Não ocorrerá período de "transição do serviço" caso não ocorra a substituição da empresa CONTRATADA ao final do período contratual.

5.14. A entrega de qualquer material/equipamento, relacionados ao objeto desta contratação, deverá ocorrer conforme as condições listadas abaixo, salvo quando definição contrária da CMB:

I. No Parque Industrial da CMB, localizado à Rua René Bittencourt, nº 371 - Distrito Industrial de Santa Cruz, CEP 23.565-200, na cidade do Rio de Janeiro/RJ;

II. Direcionados para o Departamento de TI Corporativo (DETIC);

III. Agendando previamente uma data e horário com a CMB;

IV. Em dias úteis, no horário compreendido entre 8:00h e 15:00h.

5.15. Os prazos estabelecidos neste Termo de Referência poderão ser estendidos por interesse/conveniência da CMB ou mediante justificativa razoável/plausível apresentada pela CONTRATADA, sujeita a análise e aceitação por parte da CMB;

5.16. Para um maior detalhamento das etapas previstas no cronograma apresentado na tabela **"Cronograma de Entregáveis"**, a CONTRATADA deverá observar as informações discriminadas na **"Especificação Técnica" (APENSO A)** deste Termo de Referência.

6. DO NÍVEL MÍNIMO DE SERVIÇO (NMS)

6.1. Serão aplicadas glosas à CONTRATADA, sob forma de desconto sobre o valor mensal do contrato, referentes ao não cumprimento dos indicadores estabelecidos em **"Níveis Mínimos de Serviço (NMS)" (APENSO D)** deste Termo de Referência;

6.2. Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir diversos fatores (qualidade, desempenho, disponibilidade e segurança) relacionados ao objeto contratado;

6.3. A aplicação de glosa não tem natureza de sanção administrativa, mas sim de compensação, como forma de simplificação processual;

6.4. A glosa aplicada poderá ser objeto de contestação da CONTRATADA por meio do oferecimento de elementos que visem comprovar a sua não responsabilidade;

6.5. Os indicadores serão medidos do primeiro ao último dia de cada mês e representados pelo parâmetro de valor exato (=), limite máximo (<=) ou limite mínimo (>=) que deve ser alcançado pela CONTRATADA;

6.6. O valor do desconto, decorrente da glosa, deverá ser concedido na fatura do mês de referência da prestação do serviço, em que foi identificado o não atendimento dos respectivos indicadores;

6.7. O não atingimento de um mesmo Nível Mínimo de Serviço durante 3 (três) meses consecutivos ou 5 (cinco) meses intervalados, em um período de 12 (doze) meses, ensejará a aplicação das Sanções Administrativas previstas neste Termo de Referência;

6.8. Os Níveis Mínimos de Serviço serão mensurados de forma automatizada e não poderão ser manipulados pela CONTRATADA;

6.9. O faturamento somente poderá ser emitido pela CONTRATADA e atestado pelo fiscal do contrato, após a aferição dos devidos descontos a serem concedidos.

7. DA SEGURANÇA DAS INFORMAÇÕES

7.1. A CONTRATADA deverá assinar **"Acordo de Confidencialidade" (APENSO B)** das informações que vier a ter acesso em razão da execução do contrato, com previsão das condições e obrigações a serem cumpridas durante e após a vigência do instrumento contratual;

7.2. Deverá manter a confidencialidade de todos os dados e documentos da CMB ou de terceiros, que foram produzidos, que tiver acesso ou tomado conhecimento em razão da execução do objeto desta contratação;

7.3. Não poderá, sem prévia autorização da CMB, veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato;

7.4. Os dados, metadados e informações não poderão, sob nenhuma hipótese, ser fornecidos a terceiros e/ou usados para fins diversos do previsto nesta contratação;

7.5. Não poderá acessar ou manipular qualquer dado a ela confiada sem a prévia autorização da CMB, devendo notificar imediatamente qualquer má utilização, acesso indevido, manipulação não autorizada ou qualquer outra violação que chegue ao seu conhecimento;

7.6. Todos os dados gerados, operacionalizados e custodiados pela CONTRATADA, em razão da prestação do objeto contratado, são de exclusiva propriedade da CMB, a quem deverá ser assegurado acesso irrestrito a qualquer momento durante a vigência contratual;

7.7. A CONTRATADA deverá entregar para a CMB qualquer documentação produzida em decorrência da prestação do objeto contratado, bem como ceder, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos resultados produzidos durante a vigência do contrato e eventuais aditivos;

7.8. Após do término do contrato, independente do motivo que levaram a tal, a CONTRATADA deverá garantir que a CMB possa extrair os seus dados do ambiente onde eles se encontram hospedados;

7.9. Na hipótese de a CONTRATADA receber solicitação de acesso a dados da CMB sob sua custódia, formulada por autoridade governamental, nacional ou estrangeira, deverá comunicar o fato imediatamente à CMB, ressalvadas as hipóteses legais de sigilo, quando este for expressamente exigido pela autoridade competente;

7.9.1. A CONTRATADA deverá envidar seus melhores esforços para questionar, nas esferas administrativa e/ou judicial, às suas próprias expensas, quaisquer solicitações de acesso formuladas por autoridades governamentais que não possuam inequívoco respaldo legal, antes de conceder o acesso requerido.

7.10. A CONTRATADA deverá, sempre que requisitada, comprovar a adoção e a observância das melhores práticas de segurança da informação, com vistas à mitigação de riscos que possam impactar a CMB no âmbito do objeto da contratação, bem como comunicar imediatamente a ocorrência ou a identificação de qualquer incidente de segurança da informação que possa ter afetado ou venha a afetar a CMB.

8. DAS OBRIGAÇÕES DA CMB

8.1. Nomear Gestor e Fiscais do contrato para acompanhar e fiscalizar a execução do contrato;

8.2. Receber o objeto fornecido pela CONTRATADA no prazo e em conformidade com as condições estabelecidas no Edital e da proposta, para fins de aceitação e recebimento definitivo;

8.3. Comunicar a CONTRATADA sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para devida correção;

8.4. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/empregado especialmente designado, registrando ocorrências relacionadas com a execução do objeto e determinando as medidas necessárias à regularização dos problemas observados;

8.5. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e na forma estabelecidos no instrumento contratual;

8.6. Proporcionar, quando aplicável, os recursos necessários para que a CONTRATADA possa prover com eficiência o objeto contratado;

8.7. Viabilizar, nos termos deste instrumento, o acesso dos profissionais da CONTRATADA às premissas da CMB ou de forma remota para a devida prestação do objeto contrato;

8.8. Avaliar o cumprimento da CONTRATADA dos prazos estabelecidos, aplicando penalidades quando couber;

8.9. Fornecer à CONTRATADA informações e esclarecimentos necessários quanto a execução do objeto;

8.10. Validar relatórios e planos de ação emitidos pela CONTRATADA, mantendo registro formal das aprovações;

8.11. Fornecer à CONTRATADA as autorizações necessárias para execução do objeto, garantindo que não impacte o ambiente de produção.

9. DAS OBRIGAÇÕES DA CONTRATADA

9.1. Indicar formalmente preposto que tenha capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual;

9.2. Cumprir todas as obrigações constantes no instrumento contratual, assumindo como exclusivamente seus os riscos e as despesas decorrentes da perfeita execução do objeto;

9.3. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no instrumento contratual;

9.4. Substituir, reparar ou corrigir, às suas expensas, objeto com avarias/defeitos ou em desconformidade com as exigências estabelecidas neste instrumento;

9.5. Comunicar à CMB, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.6. Manter, durante toda a vigência do instrumento contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

9.7. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

9.8. Reparar quaisquer danos diretamente causados à CMB ou a terceiros, independentemente da comprovação de culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização da execução contratual pela CMB;

9.9. Propiciar todos os meios necessários à fiscalização do contrato pela CMB, que terá poderes para sustar o fornecimento do objeto, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

9.10. Fornecer e responsabilizar-se por todos os recursos materiais e humanos necessários à execução do objeto contratado, arcando com todas as despesas de qualquer natureza;

9.11. Observar e atender a todas as normas e instruções emanadas pela CMB, além de toda a legislação pertinente;

9.12. Reportar imediatamente anormalidade, erro ou irregularidade que possa comprometer a execução do objeto;

9.13. Atender convocações da CMB de acordo com os prazos e condições estabelecidas neste instrumento contratual.

10. DA VISTORIA

10.1. Será **facultado ao licitante** vistoriar o local onde será executado o serviço, de forma a inteirar-se das condições e grau de dificuldades existentes, devendo, no ato da vistoria, assinar **"Acordo de Confidencialidade" (APENSO B)** em razão das informações que vier ter acesso;

10.2. Tendo em vista a faculdade para realização da vistoria, o licitante não poderá alegar o desconhecimento das condições e grau de dificuldades existentes como justificativa para se eximirem das obrigações assumidas ou em favor de eventuais pretensões de acréscimos de preços em decorrência da execução do objeto;

10.3. A vistoria deverá ocorrer em **até 3 (três) dias** antes do último dia útil que anteceder à data de abertura do Pregão, por meio de um representante credenciado pelo licitante, que será acompanhado por um profissional designado pela CMB;

10.4. A vistoria poderá ser realizada, de segunda à sexta-feira, na unidade Santa Cruz (Rua René Bittencourt nº 371- Distrito Industrial de Santa Cruz - Rio de Janeiro/RJ) e/ou na unidade Flamengo (Praia do Flamengo, 66 / 19º andar – Praia do Flamengo - Rio de Janeiro/RJ), no horário entre 9:00 às 15:00 horas, com duração máxima de 02 (duas) horas, devendo o agendamento ser efetuado previamente pelo endereço: seinf.segredes@cmb.gov.br;

10.5. Ao término da vistoria, o profissional designado pela CMB e o representante do licitante deverão assinar duas vias do documento **"Declaração de Vistoria" (APENSO E)**, onde uma via ficará retida e a outra será entregue ao licitante.

11. DA ACEITABILIDADE DA PROPOSTA

11.1. Encerrada a fase competitiva, caberá ao proponente detentor da melhor oferta encaminhar proposta comercial elaborada em conformidade com modelo constante em **"Proposta de Preços" (APENSO F)**;

11.2. A proposta comercial apresentada deverá ser elaborada em língua portuguesa (Brasil), com suas páginas numeradas, sem emendas, acréscimos, borrões, rasuras, ressalvas, entrelinhas ou omissões que acarretem lesão ao direito dos demais licitantes, prejuízo à CMB ou impeçam a exata compreensão de seu conteúdo. A proposta deverá contar, no mínimo, com os seguintes elementos:

I. Razão social, CNPJ, endereço completo, número de telefone e correio eletrônico (e-mail) do licitante;

II. Valores expressos em Real (R$), observando o número máximo de 02 (duas) casas decimais após a vírgula;

III. Data e assinatura do representante do licitante, com a identificação de seu nome abaixo da assinatura;

IV. Prazo de validade da proposta (mínimo de sessenta dias), a contar da data da sessão pública.

11.3. A proposta deverá apresentar, de forma clara, completa e detalhada, a especificação dos valores mensais individuais e totais referentes aos serviços executados pelo licitante, bem como de cada componente da solução tecnológica a ser fornecido (hardware, software, licenças, assinaturas, etc.), incluindo ao menos as seguintes informações:

I. Nome e modelo do componente da solução;

II. Nome do fabricante;

III. Part Number (código de identificação única do fabricante);

IV. Forma de fornecimento (on-premise, Data Center próprio do licitante, Data Center de terceiros alocado pelo licitante, Data Center de provedores de cloud públicas de mercado ou Data Center do próprio fabricante);

V. Quantidade e unidade/métrica utilizada;

VI. Valor unitário mensal do componente;

VII. Valor total mensal do componente (Quantidade × Valor unitário);

VIII. Valor do Subtotal mensal correspondente da solução.

11.4. A proposta deverá ser complementada por planilha “ponto a ponto” de comprovação do atendimento dos requisitos técnicos previstos neste instrumento, em conformidade com modelo constante em **“Comprovação de Requisitos” (APENSO G)** deste Termo de Referência;

11.4.1. Para sua devida comprovação, além dos requisitos específicos já destacados diretamente no **APENSO G**, caberá à CONTRATADA apresentar

também comprovação de todos os requisitos técnicos exigidos para as soluções tecnológicas ofertadas;

11.4.2. Para o correto preenchimento do documento disponibilizado no **APENSO G**, o proponente deverá tomar como base a seguinte orientação atinente às colunas da planilha:

VI. **ITEM:** Deve ser indicado o número do item vinculado ao requisito técnico exigido, em consonância com o disposto na seção **"Soluções Tecnológicas de Cibersegurança"** presente na **"Especificação Técnica" (APENSO A)** deste documento. Todos os itens devem ser obrigatoriamente listados para sua devida comprovação. Caso o licitante entenda que algum item não seja passível de comprovação, deverá apresentar justificativa razoável/plausível na coluna "observação", sujeita a apreciação e eventual aceitação por parte da CMB;

VII. **DOCUMENTO:** Deve ser indicado o nome do documento enviado pelo proponente, que contém o conteúdo comprobatório do requisito exigido. Este documento será utilizado pela CMB para averiguação da conformidade. Portanto, visando evitar possíveis falhas interpretativas e agilizar o processo de avaliação, recomenda-se que o proponente adote uma padronização de nomes clara e consistente para os documentos apresentados;

VIII. **PÁGINA:** Deve ser indicado o número da página do documento que contém o conteúdo comprobatório do requisito técnico;

IX. **TRECHO:** Deve ser destacado, sem modificações (ipsis litteris), segmento do texto original presente do documento oficial que comprove o atendimento satisfatório do requisito técnico exigido;

X. **OBSERVAÇÃO:** Deve ser indicado qualquer informação relevante ou complementar que possa auxiliar a CMB na correta compreensão do conteúdo comprobatório apresentado pelo licitante. Além disso, deve ser utilizado para apresentação de justificativa em caso de impossibilidade de comprovação.

11.4.3. Para fins de comprovação dos requisitos técnicos, os seguintes documentos oficiais do fabricante, relativos às soluções tecnológicas ofertadas, poderão ser apresentados:

X. Datasheet ou especificações técnicas oficiais;

XI. Guia de implementação ou manual de configuração;
XII. Documento de arquitetura da solução;
XIII. Notas de versão (release notes) da versão mais recente;
XIV. Whitepaper técnico detalhando as funcionalidades principais;
XV. Documentação de API (se aplicável);
XVI. Certificações relevantes do produto;
XVII. Documento de comparativo técnico com soluções similares;
XVIII. Artigos técnicos publicados em blog oficial do fabricante.

11.4.4. A documentação técnica poderá, caso necessário, ser disponibilizada por meio de repositório eletrônico próprio (Ex. Microsoft OneDrive, Google Drive, etc.), desde que sejam devidamente informados a URL completa, a senha de acesso (se aplicável) e assegurado que a permissão para download dos arquivos esteja ativa para a CMB;

11.4.5. Todos os documentos comprobatórios apresentados deverão ser oficiais do fabricante, não sendo aceito documentos de terceiros;

11.4.6. Não serão aceitas declarações ou cartas de conformidade ou adequação ao especificado no Termo de Referência em substituição ou complementação da documentação oficial do fabricante;

11.4.7. Serão aceitos apenas documentos em português, inglês ou espanhol para comprovação das especificações técnicas.

11.5. O fornecimento das soluções deverá englobar todos os hardwares, softwares e licenças necessários ao seu funcionamento e para o pleno atendimento das especificações técnicas exigidas, mesmo que não solicitados explicitamente neste Termo de Referência;

11.5.1. Caso o licitante necessite fornecer hardwares e/ou softwares adicionais não especificados nominalmente, mas necessários para o atendimento das funcionalidades exigidas, estes deverão estar devidamente identificados na proposta, juntamente com seus custos individuais.

11.6. A entrega dos documentos previstos nesta seção é obrigatória, tendo o objetivo de garantir a correta identificação do objeto ofertado pelo proponente. Tal exigência visa permitir à CMB uma avaliação precisa das propostas, assegurando sua integral aderência aos requisitos estabelecidos, além de prevenir a ocorrência de sobrepreços, superfaturamento ou a inclusão indevida de custos que possam resultar em pagamentos irregulares, conforme previsto no Art. 31 da Lei nº 13.303/2016;

11.6.1. A **não conformidade da proposta comercial**, seja por ausência ou inadequação aos padrões estabelecidos, poderá resultar na **desclassificação do licitante.**

11.7. A CMB poderá promover diligências diretamente com o licitante para dirimir quaisquer dúvidas, esclarecer ou complementar informações apresentadas a fim de aferir a sua veracidade, o que poderá ocorrer, a seu critério, de forma presencial, audioconferência ou e-mail.

12. DA QUALIFICAÇÃO TÉCNICA

12.1. Será **obrigatório ao licitante vencedor** apresentar um, ou mais, atestado(s) ou certidão(ões) de capacidade técnico-operacional, expedido por pessoa(s) Jurídica(s) de direito público ou privado que, na condição de cliente(s) final(is), comprove(m) o fornecimento satisfatório, pelo licitante, de serviço com características compatíveis com o objeto da licitação pelo período mínimo, sucessivos ou não, de **24 (vinte e quatro) meses**;

12.2. Os atestados apresentados deverão comprovar que a licitante tenha executado ou esteja executando serviços de características técnicas semelhantes ao objeto, relacionadas às seguintes competências:

I. Monitoramento e gerenciamento de soluções de cibersegurança;

II. Detecção e resposta de incidentes de cibersegurança em regime contínuo e ininterrupto (24×7x365), envolvendo ao menos ações relacionadas a Inteligência de ameaças (threat intelligence), caçada de ameaças (threat hunting) e gerenciamento de crises cibernéticas;

III. Gestão de vulnerabilidades de cibersegurança;

IV. Fornecimento e implementação de soluções de cibersegurança (não havendo necessidade de correspondência exata ao rol de soluções exigidas, porém devem possuir afinidade com cibersegurança);

V. Operação com Centro de Operações de Segurança (SOC).

12.3. Será permitido o somatório de atestados para efeito de comprovação de experiência na prestação do serviço, não se exigindo que todos tenham sido prestados a uma única pessoa jurídica de direito público ou privado, desde que a soma atenda o quantitativo mínimo de **1.000 (mil) ativos**, volume que corresponde a aproximadamente 50% do volume atual da CMB;

12.4. Nos atestados deverão estar expressos, no mínimo, as seguintes informações:

I. Nome e CNPJ do licitante;

II. Nome e CNPJ do cliente;
III. Descrição completa do fornecimento/serviço executado que permitam o amplo entendimento dos trabalhos realizados e identifiquem a compatibilidade e semelhança com objeto da licitação;
IV. Período de vigência do contrato;
V. Nome e e-mail do emissor do atestado;
VI. Data de emissão e assinatura do emissor.

12.5. Não serão considerados os atestados emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente ou que tenham pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da proponente;

12.6. O licitante deverá disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados ofertados na presente licitação,

podendo apresentar, dentre outros documentos, cópia do contrato que deu suporte à contratação, Notas Fiscais/Faturas, Notas de Empenho;

12.7. A CMB reserva-se o direito de diligenciar a pessoa jurídica indicada no atestado de capacidade técnica, a fim de validar ou esclarecer informações sobre o serviço prestado.

13. DO PAGAMENTO

13.1. O pagamento será efetuado e forma **mensal**, no prazo de **30 (trinta) dias consecutivos**, contados da apresentação da Nota Fiscal/Fatura contendo o detalhamento do objeto entregue, através de transferências bancárias, para crédito em banco, agência e conta corrente indicados pela CONTRATADA;

13.2. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação de qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária;

13.3. O pagamento será realizado somente após o recebimento definitivo do objeto pela CMB, desde que não se verifiquem falhas na sua execução;

13.4. O pagamento realizado será baseado em função dos resultados apresentados, ou seja, somente após mensuração, avaliação e validação dos Níveis Mínimos de Serviço (NMS) definidos, de modo a resguardar a eficiência e a qualidade na prestação do serviço.

14. DA SUBCONTRATAÇÃO

14.1. Fica vedado neste ato, à CONTRATADA, transferir, ceder, subcontratar, negociar, utilizar em qualquer hipótese como garantia ou instrumento de fiança ou caução, seja comercial ou bancária, bem como transacionar com terceiros de qualquer personalidade jurídica, as obrigações, responsabilidades e demais cláusulas estabelecidas no instrumento contratual, sem a competente, expressa e formal anuência da CMB.

15. DA ALTERAÇÃO SUBJETIVA

15.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do instrumento contratual; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do instrumento contratual.

16. DA GARANTIA DE EXECUÇÃO

16.1. Deverá ser apresentada garantia de execução do instrumento contratual, nas condições estabelecidas no instrumento contratual, correspondente a 3% (três por cento) do valor total do instrumento contratual.

17. DAS SANÇÕES ADMINISTRATIVAS

17.1. Comete infração administrativa, a CONTRATADA que:

17.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

17.1.2. Ensejar o retardamento da execução do objeto;

17.1.3. Fraudar na execução do instrumento contratual;

17.1.4. Comportar-se de modo inidôneo;

17.1.5. Cometer fraude fiscal.

17.2. A CONTRATADA que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções, nos termos da Lei nº 13.303/2016:

17.2.1. Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a CMB;

17.2.2. Multa moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite do valor total do instrumento contratual;

17.2.3. Multa de até 10% (dez por cento) sobre o valor total do instrumento contratual, no caso de inexecução total do objeto;

I. Em caso de inexecução parcial, a multa, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida.

17.2.4. Suspensão temporária de participação em licitação e impedimento de contratar com a Casa da Moeda do Brasil por até 2 (dois) anos.

17.3. O não atendimento integral ou parcial do envio da Ficha com Dados de Segurança – FDS, quando exigido, acarretará em multa de 5% (cinco por cento) sobre o valor total da Nota fiscal de entrega, podendo ser duplicada na reincidência, sem prejuízo da possibilidade de aplicação das demais penalidades previstas;

17.4. O não atendimento integral ou parcial do envio de certificados, laudos ou boletins técnicos que asseguram a qualidade dos itens garantidos pelo fornecedor, quando exigido, acarretará na aplicação das penalidades de advertência e/ou multa de até 2% sobre o valor total da Nota Fiscal de entrega, sem prejuízo da possibilidade de aplicação das demais penalidades previstas;

17.5. As penalidades de advertência e de suspensão temporária poderão ser aplicadas juntamente com a penalidade de multa;

17.6. As sanções de caráter patrimonial observarão o valor limite do instrumento contratual;

17.7. Também fica sujeita às penalidades do art. 83, III da Lei nº 13.303, de 2016, a CONTRATADA que:

17.7.1. Tenha sofrido condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

17.7.2. Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

17.7.3. Demonstre não possuir idoneidade para contratar com a CMB em virtude de atos ilícitos praticados.

17.8. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA;

17.9. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, a finalidade preventiva, o caráter educativo da pena, bem como o dano causado à CMB, observado o princípio da proporcionalidade;

17.10. Sem prejuízo da aplicação de penalidades, a CONTRATADA é responsável pelos danos causados à Administração ou a terceiros na forma disposta no artigo 76 da Lei 13.303/2016, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo órgão interessado;

17.11. As penalidades serão obrigatoriamente registradas no SICAF;

17.12. As multas previstas, quando aplicadas, deverão ser recolhidas na Seção de Tesouraria - SETES da CMB no prazo de até 10 (dez) dias úteis, contados do recebimento da notificação por correio ou outro meio qualquer que ateste o recebimento;

17.12.1. Caso não haja recolhimento no prazo indicado no subitem anterior e o valor da multa for superior ao valor da garantia prestada, quando houver, além da perda desta, responderá a CONTRATADA pela diferença, a qual será descontada dos pagamentos eventualmente devidos pela CMB ou, ainda, quando for o caso, cobrada judicialmente, nos termos dos artigos 82, §§2º e 3º e 83, §1º, da Lei nº 13.303/2016.

17.13. Não cumprida a obrigação, também responderá o contratado na forma do artigo 389 do Código Civil.

18. DA VIGÊNCIA DA CONTRATAÇÃO

18.1. O prazo de vigência da contratação é de **36 (trinta e seis) meses**, contados da assinatura do instrumento contratual, podendo ser prorrogado por iguais e sucessivos períodos ou frações, até o limite de 60 (sessenta) meses.

19. SUMÁRIO DE APENSOS

APENSO A: Especificação Técnica.

APENSO B: Acordo de Confidencialidade.

APENSO C: Termo de Aceite Definitivo.

APENSO D: Níveis Mínimos de Serviço (NMS).

APENSO E: Declaração de Vistoria.

APENSO F: Proposta de Preços.

APENSO G: Comprovação dos Requisitos.

APENSO H: Soluções Internas.

APENSO I: Modelagem dos Processos.

APENSO J: Topologias de Referência.

APENSO A - ESPECIFICAÇÃO TÉCNICA

1. REQUISITOS GERAIS

QUANTO A EXECUÇÃO DO SERVIÇO

1.1. A CONTRATADA será responsável por prover todos os recursos de infraestrutura, solução tecnológica e time especializado, nos moldes deste Termo de Referência, necessários para o pleno atendimento desta contratação, salvo quando explicitamente indicado o contrário;

1.2. Deverá acompanhar a qualidade do serviço prestado observando integralmente os Níveis Mínimos de Serviço (NMS) estabelecidos;

1.3. Deverá manter uma comunicação ativa e transparente com a CMB, fornecendo atualizações regulares sobre o andamento das atividades e quaisquer dificuldades e desafios enfrentados;

1.4. Deverá aplicar todos os controles de segurança adequados para garantir a confidencialidade dos dados da CMB que vier a receber ou ter acesso ao longo da vigência contratual;

1.5. Deverá realizar o levantamento de todas as informações necessárias para a correta entrega do objeto contratado;

1.6. Deverá desempenhar todas as atividades com total integração e sinergia, buscando sempre executá-las de forma eficiente, adaptável e orientada a resultados;

1.7. Deverá manter uma rotina de análise do mercado com o objetivo de sugerir novas tecnologias de segurança que possam ser integradas ao ambiente da CMB visando sua modernização e aprimoramento contínuo;

1.8. Deverá colaborar com a CMB no desenvolvimento de planos de ação para resolução de problemas identificados em torno do serviço prestado, além de apoiar de forma consultiva para a melhoria contínua do ambiente;

1.9. Deverá apoiar/auxiliar a CMB sempre que houver demanda por mudanças nas soluções tecnológicas, causadas por atualizações ou realocações em sua infraestrutura;

1.10. Deverá adequar a redação de documentos e relatórios gerados quanto à clareza, objetividade, detalhamento técnico e conformidade com as boas práticas e normas aplicáveis;

1.11. Deverá apresentar o planejamento de quaisquer necessidades de mudanças com potencial impacto negativo ao ambiente da CMB, realizando o mapeamento das mudanças necessárias e seus possíveis riscos;

1.11.1. Caberá à CMB, baseado no planejamento proposto, deliberar quanto a necessidade do acionamento do seu processo interno de gestão de mudanças.

1.12. Deverá dimensionar equipe técnica em quantitativo e capacitação compatíveis com as exigências da contratação, a fim de garantir que o objeto seja executado dentro dos prazos máximos exigidos e sem interrupção;

1.12.1. A CONTRATADA deverá responsabilizar-se integralmente pela equipe técnica designada para prestação do objeto, primando sempre pela sua máxima qualidade, desempenho e eficiência;

1.12.2. Os profissionais colocados à disposição da CMB, embora sujeitos às suas normas disciplinares e de segurança, não terão com ela qualquer vínculo empregatício;

1.12.3. O serviço deverá ser executado por profissionais devidamente qualificados, conforme discriminado mais adiantes neste documento.

1.13. O serviço, incluindo as suas atividades correlatas, deverá ser prestado em regime integral, **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano**;

1.14. O serviço deverá ser prestado majoritariamente de forma remota, exceto, quando requisitado pela CMB, nos seguintes casos:

I. Upgrade/downgrade de versão/firmware das soluções (somente quando o procedimento remoto falhar ou estiver impactando a CMB);
II. Configuração inicial das soluções (somente quando hospedadas nas instalações da CMB);
III. Recuperação/restauração das soluções (somente quando hospedadas nas instalações da CMB);
IV. Atuação em incidentes de cibersegurança massivos ou desastres;
V. A comunicação entre as partes esteja temporariamente prejudicada, dificultando a atuação remota para o devido cumprimento contratual.

1.15. A CONTRATADA poderá, excepcionalmente e a seu critério, solicitar a presença de seus profissionais nas dependências da CMB para atendimento de demandas técnicas ou para a correção de problemas, incidentes ou anomalias em qualquer componente da solução. Nesses casos, competirá exclusivamente à CMB avaliar e concordar com a solicitação, mediante apresentação de justificativa técnica devidamente fundamentada pela CONTRATADA;

1.16. A CONTRATADA deverá permanecer à disposição para participar, sempre que solicitado pela CMB, de reuniões remotas ou presenciais destinadas à apresentação de documentos, relatórios ou fornecimento de esclarecimentos acerca de quaisquer aspectos da contratação;

1.17. Sempre que necessária a presença de profissionais da CONTRATADA nas premissas da CMB, independentemente da sua motivação, a CONTRATADA deverá, no prazo máximo de **até 8 (oito) horas**, encaminhar previamente as seguintes informações:

I. Nome completo, número de RG e CPF dos profissionais;
II. Nome, marca e “serial number” dos equipamentos portados.

1.18. Caberá à CMB viabilizar e aprovar o acesso de todos os profissionais indicados pela CONTRATADA às suas dependências. Após a respectiva aprovação, a CONTRATADA deverá assegurar que os profissionais designados compareçam às instalações da CMB no prazo máximo de **72 (setenta e duas) horas**. O atendimento poderá ocorrer, a critério exclusivo da CMB, em qualquer uma das seguintes unidades:

I. **Unidade Santa Cruz:** Rua René Bittencourt nº 371- Distrito Industrial de Santa Cruz - Rio de Janeiro/RJ;
II. **Unidade Flamengo:** Praia do Flamengo, 66 / 19º andar – Praia do Flamengo - Rio de Janeiro/RJ

1.19. O serviço prestado deverá cobrir tanto os ambientes tecnológicos atuais das CMB, quanto os que vierem a surgir ao longo da vigência contratual, respeitados os quantitativos estabelecidos neste documento;

1.20. Não poderá haver limitadores, ao longo da vigência contratual, com relação a quantidade de demandas ou uso do serviço contratado, respeitados os quantitativos e limites estabelecidos neste documento;

1.21. Ocorrerá por conta da CONTRATADA toda e qualquer despesa, independente da sua natureza, necessárias para a correta entrega do objeto contratado;

1.22. Não poderão ser geradas cobranças adicionais para além dos quantitativos estabelecidos neste Termo de Referência, salvo na condição de aditivo contratual de interesse exclusivo da CMB (Lei 13.303 Art. 81, II c/c §1º);

1.23. Para todas as atividades executadas, deverá ser empregada a língua portuguesa falada e escrita do Brasil, salvo para uso de termos técnicos em inglês, acesso a sites com conteúdo na língua inglesa e material original do fabricante em inglês;

1.24. As soluções tecnológicas ofertadas devem obrigatoriamente atender a todas as especificações técnicas exigidas durante toda vigência contratual;

1.25. Todos os requisitos exigidos neste Termo de Referência devem ser considerados como os mínimos necessários para o devido atendimento da contratação;

1.26. A CMB (ou instituição independente por ela autorizada) poderá, a qualquer tempo ao longo do contrato, auditar a CONTRATADA a fim de averiguar o correto cumprimento dos requisitos exigidos neste Termo de Referência, cabendo inclusive visitas presenciais não programadas ao ambiente da CONTRATADA, além da solicitação do envio de documentações comprobatórias;

1.27. Demais informações relacionadas ao ambiente tecnológico da CMB, para além das já disponibilizadas ao longo de Termo de Referência, serão mantidas em sigilo e somente poderão ser disponibilizadas mediante assinatura do **"Acordo de Confidencialidade (APENSO B)"** no momento da vistoria técnica.

QUANTO AS SOLUÇÕES OFERTADAS

1.28. A CONTRATADA deverá fornecer, **comercializadas na forma de serviço**, todo o rol de soluções tecnológicas de cibersegurança exigidos neste Termo de Referência, não havendo aquisição direta de bens nesta contratação;

1.29. Todas as soluções tecnológicas ofertadas, em regra, deverão pertencer à fabricantes amplamente consolidados no mercado, não sendo aceitas soluções desenvolvidas pela própria CONTRATADA ou baseadas em softwares projetados

para uso genérico, sem a devida customização ou parametrização para atender aos requisitos específicos deste Termo de Referência;

1.29.1. Como referência de fabricantes amplamente consolidados no mercado, serão considerados estudos ou documentos de institutos de análise independente e imparcial: Gartner, Forrester, IDC e ISG Group;

1.30. Todas as soluções deverão ser **providas no modelo Software-as-a-Service (SaaS)**, salvo em situações excepcionais, nas quais poderão ser adotados outros modelos de implementação nas seguintes condições:

I. A implementação de equipamentos/componentes das soluções ofertadas nas premissas da CMB (on-premise) será admitida apenas quando explicitamente requisitado ou autorizado neste instrumento;

II. As soluções implementadas nas premissas da CMB deverão ocorrer, preferencialmente, por meio do fornecimento de “appliances físicos”, sendo admitido o uso de “appliances virtuais” (obrigatoriamente compatíveis com VMWare) apenas quando explicitamente solicitado/autorizado neste instrumento;

III. Independentemente da implementação ocorrer através de appliances físicos ou virtuais, ambos deverão ser oficialmente homologados pelos respectivos fabricantes das soluções ofertadas, não sendo aceitos equipamentos, servidores ou sistema operacional de uso genérico;

1.31. As soluções providas no modelo de Software-as-a-Service (SaaS) deverão oferecer suporte a ambientes multi-tenant, garantindo o isolamento seguro para assegurar que os dados da CMB não sejam acessados pelos demais clientes da CONTRATADA ou fabricante;

1.32. Todos os equipamentos físicos (appliance físico) instalados nas premissas da Casa da Moeda do Brasil (CMB), deverão ter seus direitos de propriedade transferidos integralmente para a CMB ao final da vigência contratual;

1.33. A data prevista pelo fabricante para descontinuidade ("end-of-life" ou similar) dos “appliances físicos” ofertados não poderá, no momento da apresentação da proposta, coincidir com o período de vigência contratual;

1.33.1. Caso algum equipamento fornecido, durante a vigência do contrato, deixe de suportar as versões mais recentes de software/firmware disponibilizadas pelo fabricante, a CONTRATADA deverá providenciar a sua substituição sem quaisquer custos adicionais para a CMB.

1.34. Para o correto fornecimento das soluções tecnológicas de cibersegurança solicitadas, a CONTRATADA poderá optar por atender funcionalidades específicas por meio da combinação de duas ou mais soluções de fabricantes distintos (ou do mesmo fabricante), desde que haja total compatibilidade entre elas e que, imprescindivelmente, as soluções complementares ofertadas atendam todos os demais requisitos de cunho genérico/agnóstico exigidos, independentemente de tratar-se de requisito de natureza técnica ou não técnica;

1.34.1. Entende-se “solução principal” como aquela capaz de atender a maioria das funcionalidades exigidas para cada solução tecnológica solicitada neste Termo de Referência, ao passo que “solução complementar” considera-se como aquela que visa atender uma ou mais funcionalidades especificas no qual a “solução principal” ofertada não tenha a capacidade de atender;

1.34.2. Supondo, por exemplo, o cenário onde a CONTRATADA optou por ofertar uma solução complementar (de mesmo fabricante ou fabricante distinto) para atender especificamente a funcionalidade de “Patch Management” solicitada dentro da especificação voltada para “Vulnerability Management Platform”. Neste caso, ambas as soluções ofertadas (principal e complementar), além de atenderem integralmente os requisitos técnicos específicos exidos para a própria funcionalidade, deverão também estar em conformidade com todos os demais requisitos genérico/agnóstico exigidos neste Termo de Referência;

1.34.3. Entende-se requisito genérico/agnóstico como aquele que poderia ser atendido por qualquer solução, ou seja, que não está atrelado a algo que só poderia ser atendido por uma solução especializada. Considerando o cenário exemplificativo exposto no subitem anterior, é compreensível que uma solução complementar ofertada (voltada especificamente para atender a funcionalidade de “Patch Management”), não tenha a capacidade de atender requisitos técnicos especializados de uma solução de “Vulnerability Management Platform”, no entanto, ainda deverá obrigatoriamente atender aos requisitos que exigem, por exemplo, “console de administração centralizada” (natureza técnica) e “pertencer à fabricantes amplamente consolidados no mercado” (natureza não técnica);

1.34.4. Este subitem visa dar maior flexibilidade à CONTRATADA na escolha das soluções a serem ofertadas, garantindo que elas não deixem de atender ao padrão de qualidade mínimo esperado pela CMB.

1.35. Para o correto fornecimento das funcionalidades solicitadas, conforme designado para cada uma das soluções tecnológicas exigidas, a CONTRATADA poderá optar por atender uma ou mais funcionalidades especificas por meio de qualquer solução ofertada nesta contratação, mesmo que tal funcionalidade não tenha sido solicitada para aquela solução em particular no Termo de Referência;

1.35.1. Supondo, por exemplo, o cenário em que a funcionalidade de “External Attack Surface Management (EASM)”, presente dentro da especificação voltada para “Cyber Threat Intelligence Platform (CTI)”, queira ser ofertada pela CONTRATADA através da solução de “Vulnerability Management Platform”. Esta ação será permitida, desde que todas as especificações técnicas exigidas para tal funcionalidade sejam integralmente atendidas;

1.35.2. Este subitem visa dar maior flexibilidade à CONTRATADA na escolha das soluções a serem ofertadas, garantindo que elas não deixem de atender ao padrão de qualidade mínimo esperado pela CMB.

1.36. Considerando que atualmente a CMB já possui um “tenant” do fabricante Trend Micro contratado (Trend Micro Vision One), no qual também será de responsabilidade da CONTRATADA seu gerenciamento (“**Soluções Internas” - APENSO H**), as seguintes premissas devem ser observadas:

I. Caso a CONTRATADA tenha interesse em ofertar produtos do fabricante Trend Micro para entrega de todas ou parte das soluções/funcionalidades solicitadas, desde que atendidas integralmente as especificações técnicas estabelecidas neste documento, deverá fazer uso do “tenant” da própria CMB;

II. Os créditos já presentes no “tenant” (adquiridos pela CMB meio de outro processo de contratação) NÃO poderão ser utilizados pela CONTRATADA para provimento do objeto desta contratação, cabendo a mesma incrementar o “tenant” com a quantidade de créditos que julgar necessário e suficientes para o pleno atendimento dos requisitos exigidos.

1.37. As soluções ofertadas deverão contar com garantia, suporte técnico e atualização constante oficiais do fabricante, compatíveis com os com níveis de serviço exigidos nesta contratação, durante toda a vigência contratual;

1.38. A CMB reserva-se o direito de realizar quaisquer configurações, instalações, integrações ou conexões nas soluções ofertadas, desde que tais ações não resultem em danos físicos ou lógicos aos equipamentos ou sistemas. Tais intervenções não serão consideradas motivo para desobrigar o CONTRATADA

do cumprimento das obrigações assumidas, nem para suspensão, limitação ou interrupção do suporte técnico ou das garantias vinculadas à solução ofertada;

1.39. As soluções ofertadas devem possuir compatibilidade e integração entre si, não sendo admitida a utilização de softwares de terceiros para viabilizar essa condição;

1.40. Não poderá haver qualquer limitador quanto a quantidade total de ações/tarefas que a CMB poderá executar em um período específico (espécie de franquia ou similar), podendo usufruir das soluções sem interrupção ou diminuição de sua performance durante todo o período da vigência contratual, desde que os quantitativos previstos sejam respeitados;

1.41. A CONTRATADA deverá fornecer acesso à base de conhecimento técnica (Knowledge Base) disponibilizada no site oficial do fabricante referente as soluções ofertadas, permitindo que a CMB obtenha conhecimento técnico detalhado das suas funcionalidades;

1.42. As soluções ofertadas deverão ser escaláveis, permitindo o ajuste da sua capacidade a qualquer tempo ao longo da vigência do contrato, o que poderá ocorrer por meio de eventuais aditivos contratuais de interesse exclusivo da CMB (Lei 13.303 Art. 81, VI, §1º);

1.43. A CONTRATADA será responsável pela instalação, configuração e capacitação (hands-on) de todas as soluções ofertadas, independente se instaladas ou não nas premissas da CMB. Quando necessária a instalação de equipamentos nas premissas da CMB, estes poderão ser instalados nos seguintes endereços:

I. **Unidade Santa Cruz:** Rua René Bittencourt nº 371- Distrito Industrial de Santa Cruz - Rio de Janeiro/RJ;

II. **Unidade Flamengo:** Praia do Flamengo, 66 / 19º andar – Praia do Flamengo - Rio de Janeiro/RJ

1.44. Todas as soluções ofertadas deverão ser implementadas, não limitando-se a estes, de acordo com os seguintes requisitos mínimos:

I. De forma “assistida”, ou seja, com o acompanhamento da CMB à todas as atividades executadas;

II. Por profissionais especializados, que possuam experiência e certificação do respectivo fabricante da solução;

III. Em sua última versão estável recomendada pelo fabricante, salvo por definição contrária da CMB;

IV. Com total redundância (quando exigido) de forma que a falha de um componente isoladamente (hardwares, cabos, fontes, etc.) não interrompa ou degrade seu funcionamento;

V. Com total integração entre si, objetivando o devido cumprimento desta contratação e a otimização dos recursos para alcançar o maior nível de proteção possível do ambiente tecnológico da CMB;

VI. Com mecanismos de autenticação integrados ao Microsoft Active Directory Domain Services (AD DS) ou Microsoft Entra ID da CMB;

VII. Com protocolos seguros (que façam uso de criptografia) para comunicação entre os diferentes componentes da solução, assim como para o acesso à sua console de administração.

1.45. O documento "**Plano de Implementação das Soluções**, conforme já discriminado ao longo deste Termo de Referência, deverá ser utilizado pela CONTRATADA para nortear todo o processo de configuração e parametrização das soluções contratadas;

1.46. Destaca-se que as tarefas listadas abaixo **não deverão ser consideradas** como condicionante para entrega das soluções. No entanto, caberá à CONTRATADA, durante toda a vigência contratual e sem qualquer limitação quantitativa, auxiliar/apoiar os profissionais da CMB no processo de instalação, integração e troubleshooting para:

I. Instalação de agentes nos desktops e servidores da CMB;

II. Parametrização de máquinas virtuais na infraestrutura interna da CMB e instalação de serviços específicos nas mesmas, necessários para o pleno funcionamento das soluções ofertadas;

III. Configuração de ativos tecnológicos presentes na infraestrutura da CMB, que não fazem parte do escopo desta contratação, visando promover a sua integração com as soluções ofertadas.

1.47. A CONTRATADA deverá tomar as ilustrações presentes em **"Topologias de Referência" (APENSO J)** como referência quanto as expectativas da CMB com relação a implementação de algumas das soluções solicitadas;

1.47.1. As topologias apresentadas têm caráter meramente ilustrativo e não representam o quantitativo exato de equipamentos a serem instalados, tampouco refletem a topologia completa da rede da CMB;

1.47.2. A forma de implementação das soluções poderá ser alterada durante a fase de planejamento, conforme conveniência da CMB ou devido a características técnicas específicas da solução ofertada.

1.48. A implementação das soluções só será considerada como "concluída", estando apta para faturamento, após a emissão do **"Termo de Aceite Definitivo" (APENSO C)** pela CMB, o que ocorrerá apenas após avaliação de que todos os requisitos deste Termo de Referência foram integralmente cumpridos pela CONTRATADA e que a solução encontra-se plenamente operacional.

QUANTO A INFRAESTRUTURA NECESSÁRIA

1.49. O serviço deverá ser provido, no mínimo, **por meio 2 (dois) Centros de Operações de Segurança (Security Operation Center - SOC) físicos redundantes**, que devem estar em pleno funcionamento na data da assinatura do contrato, de modo que a indisponibilidade de um deles não afete a continuidade do serviço prestado;

1.49.1. Os SOC's deverão estar situados no Brasil, guardando uma distância mínima de 50 km (cinquenta quilômetros) entre si, onde ao menos um deles deve estar localizado na região sudeste do país;

1.49.2. Devem possuir UPS (Uninterruptible Power Supply) que permita a continuidade da prestação do serviço na eventualidade de interrupção de curto prazo no fornecimento de energia comercial;

1.49.3. Devem possuir gerador, com acionamento automático, para situações de eventual interrupção prolongada da energia comercial, com autonomia mínima de 72 (setenta e duas) horas.

1.50. A CONTRATADA poderá manter parte de sua equipe (Níveis 2 e 3) trabalhando de forma remota. No entanto, é imprescindível garantir a presença constante de profissionais (Nível 1) fisicamente no SOC, assegurando assim o monitoramento, identificação e o tratamento ininterrupto e eficiente de todas as ameaças e incidentes de cibersegurança;

1.50.1. A CONTRATADA deve garantir que todos os dados referentes à CMB, que vier ter acesso em decorrência da contratação, sejam tratados em ambiente exclusivo do SOC, não permitindo que eles sejam copiados e/ou manipulados em dispositivos remotos (pessoais ou corporativos);

1.50.2. A equipe do SOC poderá fazer uso de ferramentas de Inteligência Artificial e automação, com o objetivo de otimizar processos e assegurar sua eficácia,

de forma a auxiliar/apoiar a execução das suas atividades, desde que não dependa exclusivamente dessas ferramentas para a devida prestação do serviço contratado.

1.51. Os SOC's deverão possuir uma estrutura mínima para garantir que os profissionais possam executar suas atividades com o máximo de eficácia e resiliência, tais como:

I. Sistema de refrigeração por ar-condicionado;
II. Mesas e cadeiras apropriadas;
III. Recursos e equipamentos tecnológicos adequados;
IV. Estrutura de vídeo centralizada para monitoramento de incidentes em tempo real (Ex. Video Wall, televisores, entre outros).

1.52. As soluções tecnológicas deverão ser hospedadas em infraestrutura de Data Center redundantes, o que poderá ocorrer, inclusive de forma híbrida, através das seguintes alternativas: (1) Data Center próprio da CONTRATADA, (2) Data Center de terceiros alocado pela CONTRATADA, (3) Data Center de provedores de cloud públicas de mercado ou (4) Data Center do próprio fabricante da solução tecnológica ofertada;

1.52.1. As soluções deverão ser implementadas de modo que a indisponibilidade de um dos Data Centers não impacte na continuidade do serviço prestado, devendo ter a capacidade de recuperar-se automaticamente de eventuais desastres, garantindo a integridade e continuidade dos acessos aos dados históricos armazenados (respeitado o período máximo de retenção especificado neste documento) e a ingestão de novos dados;

1.53. O SOC's e os Data Centers utilizados pela CONTRATADA (principal e redundante) deverão possuir controles de segurança física, de forma a assegurar a proteção das instalações, a prevenção de acessos não autorizados e a rastreabilidade dos acessos realizados aos ambientes que suportem a operação da CMB;

1.53.1. Os recursos físicos da CONTRATADA, incluindo edificações, salas, estações de trabalho, servidores e demais ativos de infraestrutura, poderão ser compartilhados com outros clientes, desde que sejam mantidos os controles de segregação, segurança e rastreabilidade necessários à proteção das informações e dos serviços da CMB;

1.53.2. Os SOC's e os Data Centers deverão contar com sistema de CFTV (Circuito Fechado de Televisão) em operação contínua, abrangendo os acessos e

áreas críticas, de forma a viabilizar a rastreabilidade das pessoas no ambiente;

1.53.3. Os SOC's e os Data Centers deverão possuir sistema de controle de acesso físico capaz de registrar, de forma individualizada, as entradas e saídas de pessoas, mediante mecanismos de autenticação baseados em biometria, reconhecimento facial ou tecnologia equivalente que assegure identificação inequívoca do indivíduo;

1.53.4. Os Data Centers deverão contar com serviço de vigilância física especializada e armada, em regime contínuo (24x7x365), destinado à proteção patrimonial e à prevenção de acessos físicos não autorizados à infraestrutura crítica de TIC;

1.53.5. Os SOC's deverão contar com serviço de vigilância física e patrimonial, em regime contínuo (24x7x365). Esta exigência poderá ser atendida por meio da estrutura de segurança patrimonial existente na edificação, condomínio corporativo ou instalação onde os mesmos estiverem localizados, dispensada a manutenção de posto ou equipe armada dedicada.

1.54. Os SOCs e Data Centers utilizados pela CONTRATADA (principal e redundante), deverão possuir certificação ISO/IEC 27001 válida no momento da contratação, cujo escopo deverá abranger os serviços objeto deste contrato, bem como as instalações e operações dos Data Centers empregados na sua execução, garantindo a conformidade com as melhores práticas de segurança da informação;

1.54.1. A validade do certificado deverá ser mantida durante todo o período de vigência do contrato, com a obrigatoriedade de renovação e apresentação das atualizações pertinentes;

1.54.2. Em caso de falha na manutenção da certificação, durante o período de vigência contratual, a CONTRATADA deverá informar imediatamente a CMB e apresentar um plano de ação para obtenção da certificação no menor tempo possível, sob o risco de aplicação de penalidades;

1.54.3. No caso de Data Centers de terceiros, sobre os quais a CONTRATADA não detenha controle direto do processo de renovação da certificação, caberá à CONTRATADA a responsabilidade de obter, junto ao provedor do serviço, todas as informações pertinentes sobre o andamento e os prazos da renovação. Caso seja constatada negligência por parte do provedor, a

CONTRATADA deverá tomar as medidas necessárias para substituí-lo, assegurando a manutenção dos padrões exigidos de segurança.

1.55. A CONTRATADA deverá possuir e manter um plano de continuidade previamente estabelecido, que comprove sua capacidade de recuperação diante de incidentes que afetem a continuidade dos serviços prestados;

1.55.1. Na hipótese de ocorrência de incidente de desastre em um dos seus ambientes redundantes, a CONTRATADA deverá restabelecer, no prazo máximo de **30 (trinta) dias úteis**, a plena conformidade com os requisitos de redundância previstos neste documento;

1.55.2. Caberá à CONTRATADA, de forma obrigatória, comprovar a ocorrência de quaisquer incidentes que resultem na indisponibilidade de seus ambientes redundantes, mediante a apresentação de documentação e evidências que comprovem a veracidade do evento;

1.55.3. A CONTRATADA deverá comprovar a adoção de todas as ações necessárias para o restabelecimento do ambiente redundante afetado, garantindo a retomada do nível de redundância exigido neste Termo de Referência.

1.56. A CONTRATADA, sempre que necessário, deverá disponibilizar sala de reunião reservada (em escritório próprio ou locação temporária), localizada na cidade do Rio de Janeiro, que possua infraestrutura mínima adequada e capacidade para comportar até 8 (oito) profissionais da CMB;

1.56.1. A sala será utilizada pela CMB de forma esporádica e temporária, **exclusivamente para situações de crise**, ou seja, apenas no caso da ocorrência de incidente de alta gravidade que incapacite/paralise/inviabilize a continuidade das operações da CMB por meio de recursos próprios;

1.56.2. A sala deverá contar com recursos videoconferência apropriados, permitindo que os profissionais da CMB possam colaborar com a CONTRATADA para discutir, investigar, planejar e executar planos de ação para recuperação do ambiente (War Room);

1.56.3. Como infraestrutura mínima adequada, entende-se: sistema de refrigeração por ar-condicionado, mesas e cadeiras confortáveis e rede WI-FI segura;

1.56.4. A sala deverá ser disponibilizada pela CONTRATADA pelo tempo necessário até que os incidentes sejam sanados ao ponto de restabelecer as operações da CMB por meio de recursos próprios.

1.57. A CONTRATADA deverá estabelecer conexão VPN IPSec Site-to-Site interligando seus SOC's (principal e redundante) ao Data Center da CMB, de forma a viabilizar o acesso ao ambiente da CMB para o gerenciamento das soluções ou devido cumprimento das exigências contratuais;

1.57.1. Os critérios de segurança a serem adotados para configuração do IPSec deverão ser combinados entre a CMB e a CONTRATADA;

1.57.2. Deverão ser estabelecidas conexões VPN IPSec Site-to-Site redundantes para ambos os SOC's, fazendo uso de links de internet pertencentes a operadoras de telecomunicações distintas;

1.57.3. A CONTRATADA deverá monitorar a disponibilidade do túnel VPN, devendo tomar ações proativas para restabelecê-lo em caso de queda;

1.57.4. Caberá à CONTRATADA implementar e manter em seus SOC's serviço de link de internet necessários para essa finalidade;

1.57.5. A CMB já possui em sua infraestrutura serviço de link de internet contratado para estabelecimento da VPN, não sendo de responsabilidade da CONTRATADA provê-los nesta contratação.

1.58. Ressalta-se que todo o arcabouço de redundâncias exigidas tem a finalidade de garantir a continuidade do serviço prestado, mesmo no caso de incidentes ou desastres, dada relevância de tais serviços para a estratégia de cibersegurança da CMB;

QUANTO A QUALIFICAÇÃO DA EQUIPE

1.59. A CONTRATADA deverá manter em seu quadro um conjunto coeso de profissionais, altamente capacitados e especializados, com qualificação plena e conhecimento técnico compatível com a complexidade do serviço a ser prestado nesta contratação. Com vistas ao atendimento dos requisitos de qualidade esperados, a CONTRATADA deverá dispor, em seu quadro técnico, de profissionais que atendam, no mínimo, aos seguintes requisitos:

I. Todos os profissionais deverão possuir diploma/certificado de conclusão, devidamente registrado, de curso de graduação de nível superior, na área de Tecnologia da Informação (ou equivalente) OU diploma/certificado de conclusão, devidamente registrado, de curso de graduação completo em qualquer área, acompanhado de curso de pós-graduação (lato ou stricto sensu) em Tecnologia da Informação (ou equivalente), expedidos por instituição de ensino reconhecida pelo Ministério da Educação;

II. 1 (um) profissional com perfil de “Gestor de SOC” (ou equivalente), com experiência de ao menos 2 (dois) anos nessa função, ao longo dos últimos 6 (seis) anos;

III. 2 (dois) profissionais com perfil de “Analista de Cibersegurança Sênior” (ou equivalente), com experiência de ao menos 2 (dois) anos nessa função, ao longo dos últimos 6 (seis) anos;

IV. 1 (um) profissional com certificação “Certified Information Systems Security Professional (CISSP)” OU “Certified Information Security Manager (CISM)” OU “Certified Information Systems Auditor (CISA)”;

V. 1 (um) profissional com certificação “Certified Ethical Hacker (CEH)” OU “Offensive Security Certified Professional (OSCP)”;

VI. 1 (um) profissional certificado nas respectivas soluções tecnológicas ofertadas, sendo aceito certificações oficiais emitidas pelo próprio fabricante (nível professional, expert, architect ou equivalente) OU diploma de treinamentos oficiais realizados junto ao fabricante ou parceiro por ele credenciado.

1.60. A CONTRATADA poderá submeter à análise outras certificações emitidas por organizações amplamente reconhecidas no mercado, desde que diretamente relacionadas à área de segurança da informação, cabendo à CMB o direito de deliberar quanto à sua aceitação;

1.61. A formação da equipe de profissionais é de exclusiva responsabilidade da CONTRATADA, não existindo restrição ou limite para o acúmulo das certificações exigidas em um mesmo profissional;

1.62. Caberá à CONTRATADA **anualmente** comprovar que está atendendo plenamente aos requisitos de qualificação exigidos neste Termo de Referência, devendo encaminhar para a CMB, em **até 30 (trinta) dias** antes da data de aniversário do contrato, os documentos comprobatórios cabíveis;

1.63. A CMB deverá ser informada caso, em algum momento, a CONTRATADA deixe de cumprir com os requisitos de qualificação exigidos;

1.64. A CONTRATADA deve prever a substituição imediata de qualquer profissional, por outro de mesmo perfil, no caso de falta, impedimentos, férias e outras questões trabalhistas;

1.65. A CMB poderá solicitar, mediante justificativa fundamentada, a substituição de profissional que não esteja atendendo aos requisitos estabelecidos ou considerado incapaz de executar os serviços na tempestividade e nível de

qualidade exigidos. Nesses casos, a CONTRATADA deverá promover a substituição no prazo a ser acordado entre as partes, assegurando a continuidade dos serviços e a indicação de novo profissional;

1.66. Em caso de desligamento ou substituição de profissionais da equipe técnica, a CONTRATADA deverá assegurar a recomposição do quadro com profissionais que atendam aos requisitos mínimos de qualificação exigidos neste Termo de Referência, no prazo máximo de **até 45 (quarenta e cinco) dias corridos**, contados da data do afastamento. Eventual necessidade de prorrogação desse prazo deverá ser devidamente justificada e previamente submetida à anuência da CMB;

1.67. A CONTRATADA, com vistas a manutenção da excelência do serviço prestado, deverá promover o contínuo desenvolvimento e aperfeiçoamento dos profissionais envolvidos na prestação do serviço. Para isso, deverá ser elaborado um **"Plano de Capacitação"**, relativo às atividades desenvolvidas nesta contratação, abrangendo mudanças/atualizações das soluções tecnológica envolvidas, dos processos executados e para atualização das melhores práticas de segurança (reciclagem profissional);

1.67.1. O "Plano de Capacitação" apresentado deverá conter o menos: a ementa das ações de capacitação, o número de horas e o cronograma previsto;

1.67.2. Será obrigatório o mínimo de **24 (vinte e quatro) horas** de treinamento anuais por profissional;

1.67.3. Na hipótese de identificação de "lacuna de competência esperada e/ou necessária" para a execução do serviço, a CMB também poderá solicitar a inclusão de ações de capacitação específicas. Considera-se como "lacuna de competência esperada e/ou necessária", a identificação pela CMB, durante a execução do serviço, do não atendimento a contento dos requisitos exigidos neste Termo de Referência.

1.67.4. A CONTRATADA ficará responsável pela execução integral do plano, que deverá ser executado ao longo do ano, não podendo prejudicar ou impactar o andamento do serviço prestado.

1.68. O "Plano de Capacitação" deverá ser apresentado no prazo máximo de **até 30 (trinta) dias corridos** antes da data de aniversário do contrato (ciclo de doze meses), devendo ser ministrado ao longo do ano subsequente;

1.68.1. No primeiro ano de contrato não haverá necessidade de capacitação;

1.68.2. Em caso de prorrogação da vigência contratual, a capacitação deverá ocorrer a partir do primeiro ano do contrato normalmente.

1.69. A CMB avaliará a execução do plano e o considerará como não executado caso o número de horas previstas e treinamentos ministrados sejam inferiores a 90% (noventa por cento) do planejado;

QUANTO AO ACOMPANHAMENTO DO SERVIÇO

1.70. A CMB acompanhará e avaliará, durante toda a vigência contratual, as atividades executadas pela CONTRATADA através de um conjunto de "Indicadores-chave de Desempenho" (Key Performance Indicators - KPIs) pré-estabelecidos individualmente para cada atividade exigida, conforme pode ser observado ao longo deste Termo de Referência;

1.70.1. A CONTRATADA deverá disponibilizar relatórios mensais (ciclos de trinta dias de contrato), no prazo máximo de **até o 5º (quinto) dia útil** do mês subsequente, das informações coletadas de KPIs referente ao período do mês anterior, devendo compor um único documento contendo todos os KPIs solicitados;

1.70.2. A CONTRATADA deverá disponibilizar relatórios anuais (ciclos de doze meses de contrato), no prazo máximo de **até o 10º (décimo) dia útil** do ano subsequente, destacando a média mês a mês dos KPIs coletados ao longo do ano, de forma a oferecer uma visão consolidada das informações e permitir uma análise mais precisa de tendências e padrões;

1.70.3. A CMB poderá solicitar, a qualquer tempo, a inclusão, alteração ou exclusão de KPIs, desde que compatíveis com o objeto contratado. Caberá à CONTRATADA apresentar avaliação técnica quanto à viabilidade de sua implementação e cronograma para disponibilização do novo indicador.

1.71. A CONTRATADA deverá disponibilizar relatórios executivos trimestrais (ciclos de noventa dias de contrato), no prazo máximo de **até o 10º (décimo) dia útil** do trimestre subsequente, voltados para a análise da alta gestão da CMB, demonstrando um panorama geral das principais informações e ações realizadas referente as atividades executadas, contendo ao menos os seguintes elementos:

I. Sumário executivo:

- **Introdução:** Breve descrição do SOC e o propósito do relatório;
- **Glossário:** Definições de termos técnicos e siglas utilizadas no relatório;

- **Principais Conclusões:** Resumo das principais descobertas e das ações significativas realizadas durante o período;
- **Recomendações:** Sugestões estratégicas baseadas nas análises do SOC.

II. Panorama Geral da Segurança:
- **Estado Atual da Segurança:** Visão geral da postura de segurança da organização;
- **Indicadores:** Principais métricas de alto nível que destaquem as informações sobre as atividades executadas.

III. Incidentes de Segurança:
- **Resumo de Incidentes Críticos:** Breve descrição dos incidentes mais significativos, incluindo impacto, resposta e resolução;
- **Classificação dos Incidentes:** Distribuição dos incidentes por tipo e por gravidade;
- **Tendências de Incidentes:** Comparação com períodos anteriores para identificar aumentos ou diminuições em certos tipos de incidentes.

IV. Ameaças e Riscos:
- **Principais Ameaças:** Resumo das ameaças mais relevantes enfrentadas durante o período, incluindo novas ameaças emergentes;
- **Origem das Ameaças:** Análise de onde as ameaças estão vindo (geograficamente e tipos de atacantes);
- **Vectores de Ataque:** Principais métodos de ataque utilizados contra a organização.

V. Eficiência e Desempenho:
- **Tempo de Resposta e Resolução:** Estatísticas sobre o tempo médio para detectar, responder e resolver incidentes.
- **Capacidades:** Informações sobre o monitoramento e a eficácia das ferramentas utilizadas.

VI. Iniciativas e Melhorias em Segurança:
- **Projetos Concluídos e em Andamento:** Descrição de projetos significativos de segurança, como a implementação de novas tecnologias ou melhorias nos processos;
- **Treinamento e Capacitação:** Resumo dos programas de treinamento e desenvolvimento profissional;

VII. Desafios e Lições Aprendidas:
- **Principais Desafios:** Descrição dos desafios enfrentados;
- **Lições Aprendidas:** Insights obtidos a partir das operações de segurança.

VIII. Recomendações e Próximos Passos:
- **Recomendações Estratégicas:** Ações sugeridas para melhorar a postura de segurança e a eficiência do SOC;
- **Planos Futuros:** Iniciativas planejadas para o próximo período, incluindo metas e cronogramas.

IX. Anexos (Se Necessário): Detalhes adicionais, gráficos, tabelas e outros dados relevantes para uma análise mais profunda.

1.72. Deverão também estar incluídos nos relatórios executivos informações detalhadas que forneçam insights sobre as principais descobertas e ações realizadas no período, padrões ou comportamentos indesejados que estão ocorrendo repetidamente, além de propostas de ações preventivas/corretivas adequadas para evitar sua continuidade ou agravamento;

1.73. Os relatórios poderão ser disponibilizados através de documento em formato PDF ou, preferencialmente, através de um portal eletrônico (dashboard), que permita o acompanhamento em tempo real dos indicadores estabelecidos;

1.73.1. O portal eletrônico deverá ser disponibilizado em nuvem, através de infraestrutura provida pela própria CONTRATADA, estando acessível via internet em regime integral (24x7x365);

1.73.2. Deverá ser acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.) fazendo uso de mecanismos seguros de criptografia e autenticação;

1.73.3. Deverá permitir ao menos a criação de 20 (vinte) usuários da CMB, permitindo a atribuição de diferentes perfis de acesso;

1.73.4. Deverá permitir a utilização de filtros que possibilitem a consulta dos dados em diferentes intervalos de tempo, devendo armazenar todas as informações geradas durante todo o período contratual;

1.73.5. Os usuários devem ser capazes de consultar, visualizar as informações em diferentes visões aplicáveis, incluindo gráficos diversos (tipo pizza, barra, linha etc.) e tabelas/listagens, bem como gerar relatórios.

1.74. A CONTRATADA deverá manter Plano de Melhoria Contínua dos serviços prestados, contemplando iniciativas voltadas ao aprimoramento dos processos,

aumento da eficiência operacional, redução do tempo de resposta, melhoria da qualidade das detecções, otimização das regras de correlação, evolução dos casos de uso e demais ações que contribuam para o aumento da maturidade dos serviços de segurança;

1.74.1. O Plano de Melhoria Contínua deverá ser revisado, no mínimo, trimestralmente, sendo seu andamento apresentado durante as reuniões previstas neste Termo de Referência.

1.75. A CMB poderá solicitar, a qualquer tempo, relatórios sob demanda referente a quaisquer informações relativas à contratação, que deverão obrigatoriamente ser disponibilizados em **até 48 (quarenta e oito) horas**;

1.76. Caberá à CONTRATADA, caso sejam identificadas pela CMB inconsistências, divergências ou erros em relação às informações apresentadas, promover sua correção no prazo máximo de **até 5 (cinco) dias úteis**, ou em prazo diverso combinado entre as partes;

1.77. A CONTRATADA deverá realizar reuniões periódicas de acompanhamento da execução contratual, visando avaliar a qualidade dos serviços prestados, o cumprimento dos níveis de serviço, os indicadores de desempenho e as oportunidades de melhoria contínua;

1.78. A CMB poderá, a qualquer tempo, auditar a metodologia utilizada pela CONTRATADA para cálculo dos indicadores de desempenho, podendo solicitar memória de cálculo, evidências operacionais e demais informações necessárias à validação dos resultados apresentados.

2. GESTÃO DAS SOLUÇÕES CIBERNÉTICAS

QUANTO A SUA DESCRIÇÃO

2.1. A CONTRATADA deverá gerenciar todas as soluções fornecidas por meio desta contratação, bem como as descritas em **“Soluções Internas” (APENSO H)** deste Termo de Referência (soluções já aquiridas e presentes no seu ambiente), visando a realização permanente de ações proativas, evolutivas e reativas voltadas para garantir a integridade, confidencialidade e disponibilidade do parque tecnológico da CMB;

2.2. A administração de todas as soluções tecnológicas ofertadas, bem como as descritas em **“Soluções Internas” (APENSO H)** deste Termo de Referência, deverá ocorrer no modelo híbrido (co-managed), ou seja, gerenciamento compartilhado entre a CMB e a CONTRATADA;

2.2.1. Caberá à CONTRATADA exercer as atividades de operação das soluções dentro dos limites estabelecidos neste instrumento;

2.2.2. A CMB deverá ter acesso administrativo a todas as soluções, limitado ao escopo dos seus dados, onde poderá atuar de forma autônoma, sem prévia autorização da CONTRATADA;

2.2.3. A CONTRATADA não poderá ter acesso administrativo a qualquer outro ativo/serviço da CMB, salvo quando concedido excepcionalmente para execução ações relacionadas a contratação, o que ocorrerá sempre de forma supervisionada e por tempo determinado.

2.3. O gerenciamento compartilhado da solução tecnológica, conforme descrito no item anterior, terá a finalidade de:

I. Permitir uma colaboração contínua e eficiente entre a CMB e a CONTRATADA, facilitando a identificação e resolução de problemas;

II. Mitigar riscos decorrentes da exclusiva dependência da CONTRATADA, uma vez que eventuais falhas ou a baixa qualidade na prestação do serviço podem prejudicar a CMB;

III. Mitigar riscos decorrentes da interrupção, transição e encerramento contratual, de modo a internalizar o conhecimento para minimizar impactos aos negócios da CMB;

IV. Facilitar a implementação de melhorias contínuas e inovações, aproveitando a expertise da CMB e da CONTRATADA para otimizar processos e tecnologias de maneira colaborativa;

V. Criar um ambiente de trabalho mais colaborativo e orientado a resultados, com foco na resolução rápida e eficaz de problemas.

2.4. Apesar das soluções listadas em **“Soluções Internas” (APENSO H)** serem de propriedade da CMB e não fazer parte deste Termo de Referência a sua aquisição e/ou renovação, será de responsabilidade da CONTRATADA monitorar, gerenciar, apresentar melhorias contínuas e integrá-las (quando tecnicamente viável) às demais soluções ofertadas nesta contratação;

2.4.1. Especificamente no que se refere ao serviço de Anti-DDoS apontado no apenso, caberá apenas à CONTRATADA interagir com as operadoras para investigar e mitigar os eventuais incidentes apontados.

2.5. A CONTRATADA deverá permitir, proporcionando um único ponto de contato, o registro e acompanhamento de chamados (tickets) por parte da CMB, relacionados ao objeto da contratação;

2.5.1. Os chamados serão destinados ao atendimento das demandas da CMB, abrangendo, entre outras atividades: requisições voltadas para análise pontual de eventos suspeitos, análise de vulnerabilidades específicas, pedido de informação e relatórios, solicitações de análises técnicas, apoio/auxílio na execução de atividades operacionais, requisição de atividades técnicas inerentes às soluções tecnológicas gerenciadas, além da solução de ações referentes a correção de falhas, indisponibilidades ou degradações da qualidade das soluções;

2.5.2. A CONTRATADA deverá realizar o gerenciamento de todo o ciclo de vida do chamado, o que abrange desde o registro inicial até o seu fechamento, incluindo o recebimento de solicitações, a categorização e priorização dos chamados, o encaminhamento para a equipe técnica apropriada, o acompanhamento do status e a comunicação sobre o progresso e a resolução;

2.5.3. A possibilidade do registro de chamados por parte da CMB não exclui a responsabilidade da CONTRATADA de tomar ações proativas, dentro do seu escopo de atuação, necessárias na resolução de incidentes ou problemas identificados.

2.6. Deverão ser disponibilizados, no mínimo, os seguintes canais de comunicação para atendimento dos chamados demandados pela CMB:

I. Sistema Eletrônico de Service Desk;

II. Linha ou central telefônica (gratuita ou com custo de ligação local);

III. Correio eletrônico (e-mail);

2.7. O **Sistema Eletrônico de Service Desk** será considerado o principal canal de atendimento para o registro e acompanhamento dos chamados, onde todo o ciclo de vida do atendimento deverá ser tratado e documentado;

2.7.1. Deve ser disponibilizado em infraestrutura da CONTRATADA, sendo acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.) por meio de protocolos seguros (HTTPS);

2.7.2. Todos os dados armazenados no sistema devem ser mantidos de forma criptografada, garantia sua confidencialidade;

2.7.3. Deve implementar mecanismos de autenticação, fazendo uso de senhas alfanuméricas fortes, nome de usuário único (auditável) e segundo fator de autenticação (Two-Factor-Authentication - 2FA);

2.7.4. Deve permitir o acompanhamento dos chamados em aberto, bem como consultar o histórico de chamados finalizados ao longo do contrato;

2.7.5. Deve gerar notificações por e-mail quando houver novas interações ou mudança no status dos chamados em atendimento;

2.7.6. Deve possuir integração com a ferramenta de monitoramento da CONTRATADA, responsável por monitorar as soluções tecnológicas gerenciadas, permitindo a abertura automática de chamados para eventuais incidentes identificados.

2.8. Será de responsabilidade da CONTRATADA manter uma base de conhecimento com todos os procedimentos operacionais pré-estabelecidos e aprovados pela CMB. Tal base deve fazer parte do Sistema Eletrônico de Service Desk, devendo estar acessível à CMB para consultas;

2.8.1. A CONTRATADA será responsável pela criação, revisão e manutenção de tais procedimentos, cabendo à CMB apenas participar como aprovador sempre que um novo procedimento for criado ou precisar sofrer alteração;

2.8.2. Deverão ser realizadas atualizações sempre que houver mudanças relevantes nos processos ou ferramentas.

2.9. A **Linha ou central telefônica** disponibilizada deverá permitir o recebimento de chamadas locais de telefone fixo e móvel de qualquer localidade do Brasil e estar vinculado a uma central de atendimento que organize as ligações em uma fila, devendo ser atendidas diretamente pela equipe do SOC;

2.9.1. Não serão aceitos, para atendimento deste requisito, números telefônicos de particulares, intermediários ou mesmo do próprio preposto do Contrato.

2.10. O **Correio eletrônico (e-mail)** disponibilizado deverá estar vinculado a um domínio registrado e de propriedade da CONTRATADA e hospedado em local que possua controles de segurança (Criptografia, Gestão de Identidade e Acesso, Atualizações Regulares, Proteções de Borda, etc.) adequados para garantir a confidencialidade dos dados da CMB;

2.10.1. O endereço de email disponibilizado deve permitir a abertura automática de chamados no Sistema Eletrônico de Service Desk ou ser uma conta compartilhada acessível apenas pela equipe do SOC;

2.10.2. Não serão aceitos, para atendimento deste requisito, cotas de e-mail hospedadas em provedores de email gratuitos ou de particulares ou mesmo do próprio preposto do Contrato.

2.11. Os canais de comunicação ofertados podem conter recursos de automação (URA, chatbot etc.) e autoatendimento implementados, mas devem **obrigatoriamente** oferecer a opção de contato direto com um atendente humano do SOC;

2.12. Para a abertura dos chamados, deverá ser mantido o registro mínimo das seguintes informações:

I. Número do atendimento (identificação única);
II. Identificação do atendente;
III. Identificação do solicitante;
IV. Data e hora da solicitação;
V. Tempo transcorrido do atendimento;
VI. Descrição da demanda.

2.13. O atendimento dos chamados deve ser iniciado por profissionais da CONTRATADA que estejam em horário de trabalho no momento do atendimento, vedado o uso do chamado “regime de plantão”, “sobreaviso” ou sistemas similares, onde o funcionário passa a trabalhar apenas quando acionado;

2.14. As solicitações de atendimento poderão ser registradas a qualquer dia e horário, tanto em dias úteis como finais de semana, feriados e pontos facultativos;

2.15. A CONTRATADA deverá possuir procedimento de escalação funcional documentado, em conformidade com as melhores práticas descritas pelo Technology Infrastructure Library (ITIL), com os seguintes níveis de atendimento:

I. **Primeiro Nível (N1):** Atendimento inicial que visa resolver demandas de baixa complexidade, além de encaminhar questões mais complexas para níveis superiores de suporte (se necessário);
II. **Segundo Nível (N2):** Envolve técnicos mais especializados para lidar com questões de complexidade moderada;
III. **Terceiro Nível (N3):** Acionado para problemas de alta complexidade, que demandam intervenção de especialistas e/ou do fabricante.

2.16. Deverá ser disponibilizada uma lista de “escalação extraordinária” para os chamados, possibilitando que a CMB acione instâncias hierárquicas superiores em situações excepcionais e de alta criticidade, quando as demandas não estiverem sendo tratadas a contento pelo canal de atendimento convencional do suporte;

2.16.1. A lista de “escalação extraordinária” deverá alcançar, no mínimo, o nível hierárquico de diretoria (ou equivalente) da CONTRATADA, contendo o

nome completo, cargo, telefone e e-mail de todos os profissionais relacionados;

2.16.2. Sempre que houver alterações nos profissionais constantes da lista de "escalação extraordinária", a CONTRATADA deverá comunicar imediatamente a CMB e disponibilizar a versão atualizada.

2.17. A CMB se reserva ao direito de solicitar que a CONTRATADA substitua excepcionalmente a solução tecnológica implementada por outra de fabricante distinto, na hipótese de haver cumulativamente as seguintes situações ao longo da vigência contratual:

I. Falhas que causem a interrupção ou degradação grave do funcionamento da solução, gerado por deficiência sistêmica da mesma e que dependa exclusivamente do fabricante para resolução;

II. Impossibilidade de implementar "Resoluções Paliativas" capazes de eliminar momentaneamente o impacto causado pelo problema;

III. Descumprimento do prazo máximo de **72 (setenta e duas) horas** para apresentação da resolução definitiva do problema. Este prazo poderá ser estendido uma única vez, por até **24 (vinte e quatro) horas**, mediante justificativa da CONTRATADA e aceitação da CMB.

2.18. Na hipótese de substituição da solução, nos moldes do item anterior, a CONTRATADA deverá disponibilizar uma nova solução com características iguais ou superiores, respeitando as exigências técnicas, de compatibilidade e integração estabelecidas neste Termo de Referência;

2.18.1. A nova solução deverá ser instalada e configurada, estando apta para plena utilização, em **até 30 (trinta) dias úteis** após formalizada a solicitação de substituição pela CMB;

2.18.2. Caso essa substituição venha ocorrer por mais de uma vez ao longo do contrato, a CONTRATADA não poderá retornar com a mesma solução de um fabricante já substituído, salvo quando: (1) não houver alternativa tecnicamente viável disponível no mercado OU (2) o problema que demandou a sua substituição à época tenha sido completamente sanado pelo fabricante;

2.18.3. Para ambas as exceções descritas no subitem anterior, a CONTRATADA deverá obrigatoriamente apresentar justificativa com embasamento técnico adequado de forma a comprovar tal situação, cabendo à CMB sua análise e aprovação.

2.19. Não poderá haver limitadores, ao longo da vigência contratual, com relação a quantidade de demandas, de horas, de atendimentos realizados ou uso do serviço contratado.

QUANTO AO SEU PROCEDIMENTO

2.20. Ao receber um chamado, a CONTRATADA deverá verificar previamente se o profissional responsável pela abertura do mesmo está autorizado pela equipe de fiscalização do contrato da CMB;

2.20.1. A CONTRATADA deverá realizar a gestão (ou permitir a gestão pela própria CMB) da base de contatos autorizados, devendo constar ao menos as seguintes informações: nome, telefone, e-mail e setor;

2.20.2. Apenas os membros da equipe de fiscalização do contrato poderão gerir a base de contatos autorizados;

2.20.3. No caso de tentativa de abertura de chamados por profissionais não autorizados, a CONTRATADA deverá comunicar imediatamente a equipe de fiscalização do contrato;

2.20.4. Não poderá haver limitação quanto ao número de profissionais da CMB autorizados a abrir chamados.

2.21. Requisições encaminhadas via e-mail ou telefone deverão ser registrados pela CONTRATADA no Sistema Eletrônico de Service Desk, complementando com as informações pertinentes e requeridas para o início do atendimento;

2.22. Compete à CONTRATADA realizar uma análise criteriosa dos chamados encaminhados pela CMB, avaliando seu grau de complexidade para identificar a necessidade de escalonamento para um nível de suporte mais apropriado, buscando principalmente priorizá-los adequadamente para garantir o devido cumprimento dos prazos estabelecidos nos **"Níveis Mínimos de Serviço" (APENSO D)** deste Termo de Referência;

2.23. Caso a resolução da demanda dependa (em parte ou no todo) da atuação da CMB, a CONTRATADA deverá modificar o status do chamado para “Pendente do Contratante” (ou similar) e registrar o prazo previsto para sua resolução (fornecido pela CMB);

2.23.1. Nesse caso, a contagem do Nível Mínimo de Serviço (NMS) será interrompida e retomará quando a(s) pendência(s) for(em) solucionada(s) pela CMB e o chamado devolvido à CONTRATADA.

2.24. Caso a resolução da demanda dependa (em parte ou no todo) da atuação do fornecedor da solução tecnológica gerenciada, a CONTRATADA deverá modificar o status do chamado para “Pendente do Fabricante” (ou similar) e registrar o prazo previsto para sua resolução (fornecido pelo fabricante);

2.24.1. Nesse caso, será tolerado o prazo máximo de **até 72 (setenta e duas) horas** para resolução da(s) pendência(s) identificada(s);

2.24.2. A CONTRATADA deverá manter no Eletrônico de Service Desk o número de identificação do chamado aberto junto ao canal oficial de suporte do fabricante, assim como mantê-lo atualizado com as interações realizadas no chamado.

2.25. Caso a resolução da demanda exija (em parte ou no todo) da atuação presencial da CONTRATADA nas premissas da CMB, a CONTRATADA deverá modificar o status do chamado para “Pendente de Visita Técnica” (ou similar), devendo obedecer aos prazos estabelecidos nos itens 1.17 e 1.18 da seção “QUANTO A EXECUÇÃO DO SERVIÇO”

2.25.1. Nesse caso, a contagem do Nível Mínimo de Serviço (NMS) será interrompida até que o técnico da CONTRATADA faça o primeiro acesso ao componente da solução instalado fisicamente na CMB.

2.26. A CONTRATADA deverá sempre justificar tecnicamente caso a resolução da demanda dependa de atuação da própria CMB, do fabricante da solução ou de ação presencial, devendo encaminhar para aprovação da CMB, antes da mudança do status do chamado, todas as informações relacionadas às pendências identificadas;

2.26.1. Uma vez aprovada a mudança do status do chamado, continuará sendo responsabilidade da CONTRATADA o acompanhamento do seu andamento, o esclarecimento de eventuais dúvidas, prestação do apoio técnico e consultivo necessário, devendo sempre observar os prazos definidos (pela CMB ou fabricante) no registro do chamado;

2.26.2. O acionamento do fabricante deverá ocorrer visando exclusivamente a análise de problemas de alta complexidade, no qual a CONTRATADA não tenha condições de atuar e demande a atuação direta do fabricante para sua resolução;

2.26.3. A contagem do Nível Mínimo de Serviço (NMS) será interrompida até que a CMB finalize a avaliação da justificativa apresentada.

2.27. Serão admitidas a adoção de “Resoluções Paliativas”, a serem adotadas temporariamente e exclusivamente para fins de redução ou eliminação do impacto causado por um problema no qual uma “Resolução Definitiva” ainda não esteja oficialmente disponível ou não seja possível;

2.27.1. Considera-se como “Resolução Definitiva” o restabelecido do serviço para seu estado de normalidade, sem qualquer restrição de desempenho ou funcionalidade, fazendo o uso de ações/atividades oficialmente recomendas pelo fabricante;

2.27.2. As “Resoluções Paliativas” só poderão ser adotadas quando devidamente justificadas pela CONTRATADA, devendo passar preliminarmente pela aprovação da CMB antes da sua implementação;

2.27.3. O uso de “Resoluções Paliativas” deverá ocorrer em caráter temporário, cabendo à CONTRATADA implementar a correta “Resolução Definitiva” assim que disponível;

2.27.4. A CONTRATADA não poderá se eximir da responsabilidade de oferecer “Resoluções Paliativa”, dentro do prazo máximo de **até 48 (quarenta e oito) horas**, mesmo quando o incidente estiver relacionado a um mal funcionamento da própria solução gerenciada.

2.28. A CONTRATADA deverá identificar, para o devido cumprimento dos chamados, possíveis riscos que possam trazer impacto ao ambiente da CMB, situação essa em que deverá encaminhar o detalhamento das mudanças necessárias e os respectivos riscos identificados para análise da CMB, que deliberará quanto a necessidade do acionamento do seu processo interno de gestão de mudanças;

2.29. Após atendida a demanda, o chamado deverá ficar por **5 (cinco) dias corridos** com status de “Resolvido” (ou similar), podendo ser reaberto pela CMB dentro deste período, caso seja entendido que tal chamado não foi atendido satisfatoriamente (independente de tratar-se de resolução definitiva ou paliativa);

2.29.1. Ao final do período designado, caso não haja nenhuma discordância da CMB, o chamado deverá ser alterado para o status “Fechado” (ou similar);

2.29.2. Em caso de reabertura do chamado, haverá a continuação da contagem do tempo de atendimento para fins de cumprimento do NMS estabelecido.

2.30. Será de responsabilidade da CONTRATADA sempre manter o registro, através do sistema eletrônico, de qualquer atividade que venha a executar, descrevendo todas as informações relevantes para o atendimento do chamado;

2.31. A modelagem do Processo de Atendimento de Chamados pode ser observada em **"Modelagem dos Processo" (APENSO I)** deste Termo de Referência;

QUANTO AS ATIVIDADES CONTÍNUAS

2.32. A CONTRATADA deverá realizar **semestralmente** uma avaliação completa do ambiente da CMB (Assessment de Segurança), com o objetivo identificar lacunas ou oportunidades de melhoria (Gap Analysis) para determinar a maturidade dos controles de segurança;

2.32.1. O Assessment de Segurança deverá ser realizado com base em um dos seguintes frameworks: NIST ou CIS Controls ou ISO/IEC 27001;

2.32.2. A CONTRATADA deverá elaborar um planejamento para o Assessment de Segurança, cabendo à CMB realizar a sua aprovação;

2.32.3. A CONTRATADA, após o levantamento das lacunas ou falhas de cibersegurança no ambiente, deverá elaborar, coordenar e supervisionar um plano de ação, em conjunto com a CMB, priorizando as falhas consideradas mais críticas;

2.32.4. A análise deverá ser conduzida por um profissional com certificação "Certified Information Systems Security Professional (CISSP)" OU "Certified Information Security Manager (CISM)" OU "Certified Information Systems Auditor (CISA)", que será responsável pela apresentação dos resultados da análise ao gestor, fiscais do contrato e gestores de TI da CMB.

2.33. A CONTRATADA deverá monitorar continuamente a disponibilidade e o desempenho (latência e throughput) das soluções gerenciadas, devendo avaliar criticamente, investigar, diagnosticar e resolver problemas de mau funcionamento, baixo desempenho ou consumo anômalo de recursos, cabendo realizar, quando necessário, intervenções proativas para evitar indisponibilidades;

2.33.1. Em caso de indisponibilidade de qualquer solução, a CONTRATADA deverá apresentar "Relatório de Indisponibilidade" detalhando, no mínimo, os seguintes aspectos:

I. **Descrição dos Motivos:** Descrição clara e objetiva das causas que levaram à interrupção ou degradação da solução;

II. **Principais Dificuldades:** Identificação dos obstáculos enfrentados durante o processo de recuperação, incluindo limitações técnicas, operacionais ou contratuais;

III. **Tempo de Recuperação:** Registro do tempo decorrido desde a identificação do evento até a restauração da solução;

IV. **Medidas Preventivas e Corretivas:** Propostas de ações que possam ser implementadas para evitar reincidência do evento e melhorar o plano de recuperação;

V. **Recomendações de Melhorias:** Sugestões para a evolução contínua do plano de recuperação da solução, destacando o que funcionou bem e o que poderia ser aprimorado no futuro.

2.33.2. Deve ser realizada o acompanhamento constante do consumo de recursos de hardware dos componentes das soluções, visando prever falhas e garantir que os equipamentos estejam operando dentro de suas capacidades ideais;

2.33.3. A CMB deverá ser informada sobre qualquer ocorrência de indisponibilidade, problemas de desempenho, mau funcionamento ou anomalias identificadas nas soluções.

2.34. A CONTRATADA será responsável pela restauração das soluções gerenciadas ao seu pleno estado de normalidade, observando os Níveis Mínimos de Serviço (NMS) estabelecidos. Deverá ser assegurada a integridade de todos os dados e configurações ativas existentes antes da indisponibilidade, sendo tolerado o máximo de **até 24 (vinte e quatro) horas** de perda de dados**;**

2.34.1. No que se refere aos componentes físicos (instalados nas dependências da CMB) ou virtuais (hospedados no ambiente de virtualização da CMB) das soluções, caberá à própria CMB a responsabilidade pela execução dos procedimentos de backup e restauração de suas configurações. Entretanto, permanecerá sob responsabilidade da CONTRATADA assegurar o pleno restabelecimento desses equipamentos ao seu estado de normalidade, bem como sua reintegração às demais soluções;

2.34.2. Os componentes físicos das soluções deverão ser substituídos sempre que apresentarem comportamento anômalo insuperáveis tecnicamente ou deixem de funcionar corretamente devido a falhas irreversíveis, o que deverá ocorrer em **até 72 (setenta e duas) horas**.

2.35. A CONTRATADA deverá executar a inclusão, exclusão e atualização de configurações e políticas de caráter geral nas soluções tecnológicas gerenciadas, em conformidade com as necessidades da CMB;

2.36. Deverá realizar e manter a integração entre as diferentes soluções gerenciadas, visando principalmente automatizar fluxos de resposta e agregar valor aos resultados obtidos;

2.37. Deverá realizar avaliações periódicas de desempenho e capacidade das soluções, emitindo recomendações de melhoria, expansão ou reconfiguração conforme a evolução do ambiente tecnológico e das necessidades da CMB;

2.38. Deverá realizar ajustes finos (tuning) nas soluções com o objetivo de otimizar suas configurações, políticas, regras de detecção e perfis de segurança visando a redução de falsos positivos e aumento da sua eficácia;

2.39. Deverá criar e customizar painéis (dashboards) e relatórios com a finalidade de apresentar os dados manipulados pelas soluções de maneira mais clara, objetiva e visualmente atrativa;

2.40. Deverá proceder com a abertura e o acompanhamento de chamados (tickets) junto ao fabricante da solução, responsabilizando-se por intermediar integralmente a comunicação entre a CMB e o referido fabricante;

2.41. Deverá auxiliar a CMB na integração das soluções gerenciadas com os serviços e sistemas corporativos existentes em seu ambiente, sempre que houver compatibilidade;

2.42. Deverá periodicamente recomendar a adoção de ações ou a implementação de funcionalidades relevantes, com o objetivo de promover o aprimoramento contínuo do ambiente;

2.43. Deverá manter a CMB continuamente informada acerca de quaisquer mudanças ou inconsistências relevantes identificadas no ambiente;

2.44. Deverá realizar a análise dos logs e eventos gerados pelas soluções, para fins de auditoria e troubleshooting relacionados à sua configuração, atualização, funcionamento e segurança;

2.45. Deverá realizar o gerenciamento dos alarmes e notificações geradas pelas soluções gerenciadas;

2.46. Deverá elaborar e implementar políticas de segurança com a finalidade de garantir a confidencialidade, autenticidade e disponibilidade do ambiente;

2.47. Deverá realizar análises periódicas das políticas de segurança aplicadas, a fim de garantir que permaneçam relevantes, eficazes e alinhadas aos requisitos de segurança e conformidade da CMB;

2.48. Deverá assegurar que as soluções permaneçam em conformidade com as melhores práticas do mercado e com as recomendações do fabricante;

2.49. Deverá realizar a gestão de segurança das soluções, adotando metodologias adequadas para proteger suas informações e restringir o acesso de usuários;

2.50. Deverá periodicamente revisar as credenciais dos usuários e aplicações, revogando acessos inativos ou desnecessários, além de avaliar o ajuste do seu nível de privilégio;

2.51. Deverá atualizar o sistema/firmware das soluções (incluindo patches, correções e novas versões ou releases), mantendo-as na versão mais segura e estável recomendada pelo fabricante;

2.52. Deverá atuar proativamente diante de falhas nos controles de segurança ou na ocorrência de situações não previstas que possam comprometer a integridade, disponibilidade ou confidencialidade do ambiente da CMB;

2.53. Deve gerenciar os agents instalados (quando aplicável), monitorando seu status, conectividade e versão desatualizada;

2.54. Deverá apoiar auditorias internas e externas fornecendo evidências, registros e relatórios detalhados das atividades desenvolvidas;

2.55. Deverá realizar a integração das fontes de dados (ativos monitorados) da CMB com a solução de Incident Management Platform, assegurando interoperabilidade, consistência e integridade das informações coletadas. A integração deverá contemplar, no mínimo, as seguintes atividades:

I. Definir o método de coleta de dados, considerando os tipos de ativos, as interfaces disponíveis e os protocolos suportados (por exemplo, Syslog, API REST, SNMP, agentes locais, entre outros), observando requisitos de segurança, desempenho e compatibilidade com a arquitetura da CMB;

II. Estabelecer os procedimentos operacionais necessários para a coleta, incluindo a definição de atributos, parâmetros e credenciais a serem habilitados, bem como políticas de autenticação, compressão e criptografia de dados durante o transporte;

III. Normalizar, correlacionar e realizar o parsing dos dados, logs e alertas capturados, configurando os conectores e parsers adequados para mapear os dados em um formato padronizado e compatível com o modelo de dados da plataforma de gestão de incidentes, assegurando coerência e rastreabilidade das informações;

IV. Implementar e validar todas as configurações necessárias para habilitar a coleta dos dados, incluindo testes de conectividade, validação de

credenciais, verificação de integridade dos dados e confirmação do fluxo de envio;

V. Definir, em conjunto com a CMB, o método mais eficiente e seguro para a coleta de dados, considerando aspectos de desempenho, disponibilidade e impacto na rede, de modo a não comprometer a operação dos sistemas monitorados;

VI. Manter documentação técnica sobre as integrações realizadas, contendo detalhes sobre os conectores, protocolos, formatos de dados, parâmetros configurados e eventuais dependências técnicas, de forma a garantir rastreabilidade e facilitar manutenções futuras.

2.56. Deverá monitorar e realizar revisões periódicas das fontes de dados e dos alertas gerados, verificando se estão funcionando corretamente, aplicando ajustes e correções quando necessário, e acionando a CMB sempre que a fonte afetada estiver fora do seu escopo de administração;

2.57. Deverá monitorar e garantir a sincronização temporal (timestamps) de todos os logs e eventos coletados, assegurando a consistência temporal dos registros, de forma a evitar impactos na correlação, investigação e reconstrução dos incidentes;

2.58. É vedada a exclusão ou descarte de quaisquer logs, eventos ou registros de segurança antes do término do período de retenção definido pela CMB, salvo mediante autorização formal e expressa da mesma. Qualquer solicitação de exclusão, antes do prazo de retenção, deverá ser documentada, registrada e validada pela CMB previamente à execução;

2.59. Deverá, sempre que necessário, tomar ações relacionadas aos alertas e eventos detectados, incluindo a criação de filtros e scripts personalizados, a adição de tags e comentários, o envio de notificações por e-mail e a definição de políticas de bloqueio;

2.60. Deverá realizar a criação, edição, manutenção e teste de conectores baseados em API, com o propósito de viabilizar integrações entre sistemas;

2.61. Deverá criar, revisar e aprimorar continuamente os casos de uso e as regras de correlação de eventos, com o objetivo de gerar alertas precisos e acionáveis sobre possíveis incidentes de segurança, alinhados às necessidades específicas, políticas e requisitos de monitoramento da CMB;

2.61.1. Consideram-se necessidades específicas aquelas relacionadas à definição e ao refinamento de critérios, indicadores e padrões de detecção que

considerem o contexto operacional da CMB, os ativos críticos, o ambiente tecnológico, os níveis de risco aceitáveis e os perfis de ameaças mais relevantes;

2.61.2. As regras de correlação e os casos de uso deverão ser atualizados periodicamente para incorporar novas ameaças, técnicas, táticas e procedimentos (TTPs) identificados por fontes de Threat Intelligence, bem como vulnerabilidades emergentes e mudanças na arquitetura ou nos processos da CMB, garantindo assim a eficácia contínua da detecção e resposta a incidentes;

2.61.3. As métricas de desempenho e qualidade de detecção deverão ser avaliadas e ajustadas continuamente, com foco na redução de falsos positivos e negativos, no aumento da precisão dos alertas e na otimização do tempo médio de detecção (MTTD);

2.61.4. A lógica de detecção deve ser desenvolvida e ajustada com base na utilização de múltiplos eventos e diferentes fontes de dados;

2.61.5. A inclusão, modificação ou exclusão de casos de uso e regras de correlação deverá ocorrer mediante aprovação formal da CMB, acompanhada de documentação que descreva os objetivos, critérios de detecção, impacto esperado e eventuais dependências técnicas.

2.62. Deverá criar, revisar e manter atualizados os “playbooks” de segurança cibernética com o objetivo de automatizar, simplificar, padronizar e agilizar as tarefas operacionais, garantindo respostas consistentes e eficazes aos diferentes tipos de incidentes e eventos de segurança;

2.62.1. Os “playbooks” devem conter procedimentos detalhados, instruções passo a passo e orientações claras, contemplando critérios de acionamento, fluxos de decisão e dependências;

2.62.2. Devem ser projetados de forma modular e flexível, permitindo rápida adaptação a mudanças de cenário, novas ameaças, atualizações de ferramentas, políticas internas ou requisitos regulatórios;

2.62.3. A implementação, alteração ou exclusão de qualquer “playbook” deverá passar obrigatoriamente por aprovação prévia da CMB, com registro formal das alterações realizadas e justificativas técnicas.

2.62.4. Deve ser estabelecido um ciclo periódico de revisão dos “playbooks”, garantindo sua aderência às melhores práticas, à evolução tecnológica e às lições aprendidas.

2.63. Deverá executar, de forma contínua, atividades de monitoramento, avaliação, operação e sustentação relacionadas à solução de Network Packet Broker (NPB), visando a identificação de falhas, anomalias ou degradações;

2.63.1. Deve garantir a entrega otimizada, segura e controlada do tráfego de rede às ferramentas de análise apropriadas;

2.63.2. Deve realizar o gerenciamento contínuo das políticas de filtragem, agregação, replicação e balanceamento de tráfego configuradas, assegurando que o tráfego entregue às ferramentas de análise seja relevante e sem duplicidade;

2.63.3. Deve monitorar permanentemente a solução de modo a identificar gargalos, falhas ou saturações de tráfego que possam impactar a visibilidade ou a efetividade das ferramentas de análise;

2.63.4. Deve revisar periodicamente as regras de filtragem, mascaramento, truncamento e desduplicação de pacotes, garantindo que estejam atualizadas conforme mudanças na topologia de rede, novos serviços implantados e evolução das ameaças;

2.63.5. Deve validar continuamente a integridade dos fluxos de tráfego encaminhados às ferramentas de análise, verificando se os pacotes entregues mantêm consistência temporal e se não há perda, truncamento indevido ou ordenamento incorreto de pacotes;

2.63.6. Deve apoiar a CMB na identificação e priorização de novas fontes de tráfego a serem integradas à solução, de forma a expandir gradualmente a cobertura de visibilidade da rede e aumentar a eficácia da detecção de ameaças;

2.63.7. Deverá ser utilizado para auxiliar nas atividades de correlação e investigação conduzidas pelo SOC, fornecendo dados de tráfego e estatísticas para subsidiar análises, identificação de padrões anômalos e reconstrução de eventos de segurança.

2.64. Deverá executar, de forma contínua, atividades de monitoramento, avaliação, operação e sustentação relacionadas à solução de Cyber Threat Intelligence (CTI), visando a identificação de falhas, anomalias ou degradações;

2.64.1. Deverá monitorar fontes de Threat Intelligence reconhecidas, confiáveis e continuamente atualizadas, a fim de gerar conhecimento fundamentado em evidências, tendências, contexto, técnicas, indicadores e motivações de possíveis ameaças cibernéticas. Esse conhecimento deverá apoiar a

prevenção, detecção, resposta, remediação e mitigação de riscos cibernéticos que possam impactar o ambiente tecnológico da CMB

2.64.2. Deve propor contramedidas, recomendações e executar ações proativas para mitigar riscos e reduzir a exposição cibernética da CMB, com base nas informações obtidas;

2.64.3. Deve realizar o monitoramento contínuo da superfície de ataque externa da CMB, identificando novos ativos expostos, configurações incorretas, vulnerabilidades abertas à internet, domínios e subdomínios não catalogados, certificados expirados e outros vetores de risco passíveis de exploração;

2.64.4. Deve coletar, correlacionar e enriquecer informações provenientes de alertas das soluções de segurança, com dados obtidos de CTI e outras fontes, a fim de validar ou descartar falsos positivos e apoiar investigações conduzidas pelo SOC;

2.64.5. Deve monitorar ameaças e eventos globais dominantes, incluindo atores de ameaça, campanhas ativas, vulnerabilidades críticas (CVE), malwares, ransomwares, botnets, phishing, spams, e incidentes de vazamento de informações que possam afetar a CMB direta ou indiretamente;

2.64.6. Deve monitorar ameaças direcionadas a setores, tecnologias ou regiões específicas, correlacionando-as com o contexto da CMB, de forma a antecipar ataques e reforçar defesas preventivas;

2.64.7. Deve monitorar ameaças emergentes (zero-day), novas técnicas, táticas e procedimentos (TTPs) de ataque, bem como padrões de comportamento de grupos criminosos, propondo ajustes imediatos aos controles e processos internos de segurança;

2.64.8. Deve monitorar e proteger a reputação da marca da CMB, identificando uso indevido, falsificação de identidade visual, domínios fraudulentos (typosquatting), perfis falsos em redes sociais, campanhas de phishing e demais ameaças que comprometam a imagem institucional;

2.64.9. Deve monitorar riscos à cadeia de suprimentos da CMB, incluindo fornecedores, parceiros e prestadores de serviço críticos, analisando vulnerabilidades conhecidas, incidentes públicos, exposições de dados e histórico de conformidade, com o objetivo de prevenir impactos indiretos ao ecossistema da CMB;

2.64.10. Deve alimentar continuamente as plataformas de segurança da CMB com Indicators of Compromise (IoCs) e Indicators of Attack (IoAs) identificados, permitindo aprimorar a eficácia dos seus mecanismos de detecção e resposta;

2.64.11. Deve integrar as informações obtidas aos fluxos operacionais do SOC, garantindo que sejam utilizadas para priorização de incidentes, análise de impacto e recomendações estratégicas;

2.64.12. Deve notificar a CMB sobre eventos cibernéticos relevantes, com possibilidade de configurar critérios específicos de monitoramento, níveis de alerta e priorização conforme o risco e a criticidade do ativo ou serviço afetado;

2.64.13. Deverá produzir **relatórios quinzenais** sobre tendências globais e setoriais de ameaças, vulnerabilidades críticas, indicadores de exposição, ataques recentes e recomendações específicas para o ambiente da CMB, podendo incluir painéis dinâmicos (dashboards) e análises de risco contextualizadas.

2.65. Deverá adotar todas as medidas necessárias para solicitar e acompanhar a remoção (takedown) de conteúdos considerados fraudulentos, maliciosos, falsos, difamatórios ou que possam representar risco à imagem institucional, à segurança ou aos ativos digitais da CMB;

2.65.1. Deve subsidiar a CMB com todas as informações e evidências relevantes que fundamentem o pedido de remoção, incluindo capturas de tela (screenshots), URLs, domínios, metadados, datas de detecção, relatórios técnicos e demais elementos comprobatórios do conteúdo identificado como fraudulento ou malicioso;

2.65.2. Deve tomar todas as providências cabíveis para garantir a efetividade do processo de “takedown”, incluindo, mas não se limitando a:

I. Reiteração de solicitações junto a provedores, registradores de domínio, plataformas de redes sociais e órgãos competentes;

II. Acompanhamento de respostas e prazos de atendimento;

III. Obtenção de esclarecimentos adicionais quando necessário;

IV. Acionamento de canais alternativos de contato para assegurar a remoção.

2.65.3. Deve acompanhar integralmente o ciclo de vida de cada solicitação de remoção, desde a detecção inicial até a efetiva retirada do conteúdo,

mantendo a CMB continuamente informada sobre o andamento, status, evidências de remoção e eventuais dificuldades encontradas;

2.65.4. Deve realizar o monitoramento contínuo e periódico dos canais, domínios, mídias e plataformas previamente identificados, com o objetivo de detectar possíveis reincidências ou reaparições de conteúdos semelhantes ou derivados dos que foram alvo de “takedown”, adotando novas ações corretivas, quando aplicável;

2.65.5. Deve manter histórico completo de todas as ações de “takedown” realizadas, incluindo registros de comunicação com terceiros, relatórios de execução e resultados obtidos, disponibilizando tais informações à CMB sempre que solicitado.

2.66. Deverá executar, de forma contínua, atividades de monitoramento, avaliação, operação e sustentação relacionadas à solução de Vulnerability Management Platform, visando a identificação de falhas, anomalias ou degradações;

2.66.1. Deve identificar, avaliar, priorizar e tratar vulnerabilidades que possam impactar a segurança cibernética da CMB;

2.66.2. Deve avaliar continuamente a eficácia dos processos de correção e mitigação aplicados, identificando falhas recorrentes ou ineficiências nos controles implementados;

2.66.3. Deve apoiar a CMB na definição de políticas e janelas de manutenção seguras para aplicação de correções e atualizações críticas;

2.66.4. Deve manter atualizados os perfis de varredura e os mecanismos de detecção da plataforma, garantindo a aderência às melhores práticas e aos novos vetores de vulnerabilidade;

2.66.5. Deve propor planos de ação e recomendações à CMB, visando reduzir riscos e aumentar a resiliência da infraestrutura tecnológica;

2.66.6. Deve realizar análises comparativas entre ciclos de varredura, de modo a identificar tendências, reincidências e vulnerabilidades recorrentes;

2.66.7. Deve criar, revisar e atualizar scans templates (perfis de varredura) conforme os diferentes tipos de ativos, sistemas operacionais, aplicações e níveis de profundidade de análise;

2.66.8. Deve configurar credentials-based scans (varreduras autenticadas) para ativos internos e externos, garantindo a coleta detalhada de vulnerabilidades de sistema e aplicações;

2.66.9. Deve executar varreduras sob demanda ou agendadas (scheduled scans) de acordo com políticas definidas pela CMB, controlando janelas de execução para evitar impacto operacional;

2.66.10. Deve validar a integridade e completude dos resultados das varreduras, verificando falhas de autenticação, timeouts, falsos positivos e ativos não alcançados;

2.66.11. Deve customizar parâmetros de detecção e políticas de varredura conforme o nível de criticidade dos ambientes (Ex. produção, homologação e desenvolvimento);

2.66.12. Deve configurar regras de exceção ou supressão temporária (vulnerability exceptions / false positives) devidamente justificadas e aprovadas pela CMB;

2.66.13. Deve criar asset groups e tags na solução, organizando os ativos por categoria, criticidade, localização ou unidade responsável, para facilitar a priorização de tratamento;

2.66.14. Deve gerenciar credenciais armazenadas na plataforma (por exemplo, senhas de varredura autenticada), garantindo o uso seguro, rotatividade e conformidade com políticas de acesso.

2.67. Deverá executar, de forma contínua, atividades de monitoramento, avaliação, operação e sustentação relacionadas à solução de Breach and Attack Simulation (BAS), visando a identificação de falhas, anomalias ou degradações;

2.67.1. Deve monitorar e avaliar a postura de segurança cibernética da CMB, testando ativamente a eficácia dos controles para identificar lacunas de segurança e fortalecer as defesas contra ameaças;

2.67.2. Deve realizar simulações de ataques de forma periódica, objetivando validar, testar e aprimorar a eficácia dos controles de segurança, identificar vulnerabilidades, riscos, falhas de detecção e resposta;

2.67.3. Deve executar simulações para identificar possíveis caminhos de ataque que um invasor poderia utilizar para comprometer o ambiente devido a existência de vulnerabilidades ou configurações incorretas;

2.67.4. Deve avaliar os resultados das simulações de ataques, visando promover a melhoria contínua do ambiente, devendo ao menos:

I. Identificar conjuntos de regras, correlações e detecções que estejam ausentes, redundantes, conflitantes ou obsoletas, afetando a capacidade de detecção e resposta do SOC;

II. Detectar eventos de segurança que não estejam gerando os alertas correspondentes, identificando falhas de cobertura nos mecanismos de detecção e correlação de eventos;

III. Verificar a existência de atrasos ou perdas entre a ocorrência de eventos de segurança e a geração, correlação ou notificação de alertas pela plataforma de gestão de incidentes;

IV. Assegurar que alertas, logs e dados de telemetria sejam transmitidos, armazenados e processados de forma íntegra, completa, sincronizada e consistente entre os componentes do ecossistema de segurança;

V. Identificar novas fontes de dados e telemetria necessárias para ampliar a visibilidade do ambiente e eliminar lacunas de monitoramento e cobertura;

VI. Verificar se os registros de log apresentam granularidade, contexto e enriquecimento adequados, permitindo a correlação eficaz e a investigação forense detalhada;

VII. Avaliar a eficácia e precisão das regras de monitoramento, detecção e resposta, buscando reduzir a ocorrência de falsos positivos e falsos negativos, e garantindo a correta captura e análise pelas ferramentas de segurança adequadas;

VIII. Gerar relatórios executivos e técnicos com métricas de desempenho, tendências e recomendações de melhoria contínua, permitindo a priorização de ações corretivas e a evolução do programa de cibersegurança

2.67.5. Deve realizar recomendações de ações corretivas e preventivas visando elevar de forma contínua a postura de segurança cibernética da CMB, com base nas evidências identificadas durante as simulações. Tais recomendações deverão:

I. Abranger ajustes em configurações, revisões de regras, aprimoramentos de políticas de segurança, reforço de controles de acesso, atualização de assinaturas, e otimização dos fluxos de resposta a incidentes;

II. Ser apresentadas de forma estruturada, priorizadas conforme criticidade e impacto para o ambiente da CMB, e acompanhadas de justificativas técnicas e evidências que sustentem as propostas de mitigação;

III. Propor ações de capacitação e conscientização voltadas à equipe técnica e de resposta a incidentes, quando identificado que falhas humanas, lacunas de processo ou deficiências de conhecimento contribuíram para os riscos ou vulnerabilidades detectadas;

IV. Ser documentadas em relatórios técnicos, permitindo à CMB acompanhar a evolução do nível de maturidade em segurança, bem como o progresso das medidas adotadas ao longo do tempo.

2.67.6. Deve identificar os ativos corporativos críticos, visando a elaboração de simulações de ataques personalizadas;

2.67.7. Deve avaliar a eficácia das soluções de segurança existentes no ambiente da CMB, de forma a identificar falhas e pontos de melhorias;

2.67.8. Deve buscar otimizar a eficácia das detecções e alertas, visando reduzir o Tempo Médio para Detecção (Mean Time To Detect - MTTD) e o Tempo Médio de Reparo (Mean Time to Repair - MTTR);

2.67.9. Deve conduzir ações de caça a ameaças (threat hunting), baseadas nas técnicas de simulação de ataque que se mostrem bem-sucedidas, de forma a identificar ataques reais que possam ter usado métodos semelhantes e permanecerem sem detecção.

2.68. Deverá executar, de forma contínua, atividades de monitoramento, avaliação, operação e sustentação relacionadas à solução de Security Service Edge (SSE), visando a identificação de falhas, anomalias ou degradações;

2.68.1. Deve monitorar continuamente tentativas de acesso a aplicações corporativas, identificando comportamentos anômalos e padrões suspeitos;

2.68.2. Deve gerenciar políticas de acesso baseado em identidade, contexto, dispositivo e postura de segurança;

2.68.3. Deve monitorar métricas de latência e disponibilidade dos túneis ZTNA para garantir desempenho adequado;

2.68.4. Deve gerenciar e revisar periodicamente regras de firewall e políticas de segmentação;

2.68.5. Deve manter listas de bloqueio (blacklists) e permissão (whitelists) atualizadas;

2.68.6. Deve inspecionar continuamente o tráfego web, garantindo a aplicação de políticas de filtragem de conteúdo, reputação e categorias de sites;

2.68.7. Deve monitorar downloads e uploads de arquivos em busca de malware, scripts e macros maliciosas;

2.68.8. Deve ajustar políticas de navegação conforme necessidades organizacionais e perfis de risco;

2.68.9. Deve manter atualizadas as assinaturas de ameaças e mecanismos de categorização de URLs.

2.69. Deverá executar, de forma contínua, atividades de monitoramento, avaliação, operação e sustentação relacionadas à solução de Web Application Security Platform, visando a identificação de falhas, anomalias ou degradações;

2.69.1. Deve acompanhar o desempenho, disponibilidade e segurança das aplicações web e APIs publicadas, utilizando os recursos da plataforma para identificar falhas, anomalias ou degradações de serviço;

2.69.2. Deve assegurar a proteção das aplicações web e APIs expostas, validando autenticações, controles de acesso, limitação de requisições (rate limiting) e monitoramento quanto ao uso indevido;

2.69.3. Deve monitorar continuamente indicadores de latência, erros, volume de requisições e taxas de bloqueio, com o objetivo de garantir a operação eficiente e segura dos serviços publicados;

2.69.4. Deve criar, revisar e atualizar perfis de aplicação e políticas de inspeção, assegurando sua compatibilidade com aplicações em produção e novos serviços publicados;

2.69.5. Deve acompanhar e analisar métricas de balanceamento, verificando a correta distribuição de tráfego entre os sites, a fim de assegurar alta disponibilidade e baixa latência;

2.69.6. Deve operar e ajustar as políticas de balanceamento, configurando métodos de balanceamento e parâmetros de health check;

2.69.7. Deve gerenciar as zonas DNS sob responsabilidade da plataforma, configurando registros (A, AAAA, CNAME, MX, TXT, etc.) e monitorando consultas e resoluções anômalas;

2.69.8. Deve monitorar os registros e estatísticas do serviço de DNS, incluindo consultas, resoluções e tempos de resposta, identificando variações anômalas que possam indicar falhas ou ataques;

2.69.9. Deve verificar periodicamente a integridade e validade das chaves e assinaturas DNSSEC, assegurando que os domínios permaneçam devidamente autenticados e protegidos;

2.69.10. Deve administrar e validar as configurações de DNSSEC e o monitoramento da cadeia de confiança para evitar falhas de assinatura.

2.70. Deverá executar, de forma contínua, atividades de monitoramento, avaliação, operação e sustentação relacionadas às identidades/credenciais gerenciadas pela solução de Unified Identity Security Platform, visando a identificação de falhas, anomalias ou degradações;

2.70.1. Deve monitorar continuamente todas as sessões privilegiadas, identificando comportamentos anômalos ou atividades fora do padrão;

2.70.2. Deve revisar periodicamente as permissões e identidades/credenciais privilegiadas, garantindo a aderência ao princípio do menor privilégio;

2.70.3. Deve validar a rotação e expiração automática de identidades/credenciais conforme políticas de segurança;

2.70.4. Deve revisar e ajustar periodicamente as políticas de controle de acesso, conforme as necessidades e mudanças operacionais da CMB;

2.70.5. Deve auditar o cumprimento de fluxos de aprovação para concessão de acessos privilegiados;

2.70.6. Deve monitorar e controlar a elevação de privilégios locais em estações de trabalho e servidores, detectando e bloqueando tentativas de execução de comandos administrativos não autorizados;

2.70.7. Monitorar o uso de cofres pessoais para armazenamento de senhas e credenciais, garantindo conformidade com políticas institucionais;

2.70.8. Configurar portais de acesso remoto seguro para fornecedores/terceiros, além de atualizar lista de fornecedores autorizados e revisar suas permissões de acesso privilegiado.

2.71. Deverá manter a CMB constantemente informada sobre quaisquer mudanças ou inconsistência relevantes identificadas no ambiente.

QUANTO AOS SEUS INDICADORES-CHAVE (KPI'S)

DENOMINAÇÃO	DESCRIÇÃO
Quantitativo de chamados em aberto	Número total de chamados que estão em processo de atendimento. Percentual (%): por tipo e severidade.
Quantitativo de chamados pendentes	Número total chamados com status de pendente (seja do fornecedor ou da CMB), Percentual (%): por tipo e severidade.

Quantitativo de chamados sem resolução	Número de chamados sem resolução. Percentual (%): por tipo e severidade.
Quantitativo de chamados resolvidos	Número total chamados resolvidos. Percentual (%): por tipo e severidade.
Tempo médio para resposta inicial dos chamados	Tempo médio entre a abertura do chamado até a sua primeira resposta. Percentual (%): por tipo e severidade.
Tempo médio de resolução dos chamados	Tempo médio entre a abertura do chamado até a sua resolução definitiva. Percentual (%): por tipo e severidade.
Percentual de resolução dos chamados	Percentual (%) dos chamados resolvidos em relação ao número total de chamados demandados (por tipo e severidade).
Percentual de reabertura dos chamados	Percentual (%) de chamados que foram reabertos após serem marcados como resolvidos (por tipo e severidade).
Percentual de resolução no primeiro contato	Percentual (%) de chamados que foram resolvidos logo na primeira interação, sem necessidade de retornos ou escalonamentos (por tipo e severidade).
Percentual de chamados escalonados	Percentual (%) de chamados transferidos para um nível superior de suporte (N2 ou N3).
Percentual de cumprimento do NMS	Percentual (%) de chamados resolvidos dentro do prazo estipulado no Nível Mínimo de Serviço (NMS).

3. GESTÃO DE INCIDENTES CIBERNÉTICOS

QUANTO A SUA DESCRIÇÃO

3.1. A CONTRATADA será responsável por monitorar e avaliar, de forma proativa e permanente, todo o ambiente tecnológico da CMB, visando detectar e responder possíveis ameaças e incidentes de cibersegurança, de forma a mitigar riscos que possam afetar a disponibilidade, integridade ou confidencialidade dos dados e/ou sistemas corporativos;

3.2. Deverão ser empregadas atividades voltadas para coletar e correlacionar log's gerados por múltiplas fontes de dados, visando detectar, priorizar e responder incidentes cibernéticos e atuar proativamente sobre ameaças globais ativas e emergente por meio do monitoramento de fontes reconhecidas e confiáveis de

Inteligência de Ameaças (Threat Intelligence), além de monitorar o uso indevido da marca da CMB, promovendo inclusive ações de takedown (pedido de remoção do conteúdo) quando demandado;

3.3. Para a execução adequada dessa atividade, deverá ser tomada como base as fases listadas abaixo, que juntas compõem o "Ciclo de Vida de Gestão de Incidentes" a ser executado pela CONTRATADA:

I. **PREPARAÇÃO (PREPARATION):** Fase inicial no qual deverá ser garantido que a CMB esteja pronta para responder a incidentes de segurança de maneira eficaz, através do levantamento de informações cruciais para o correto funcionamento do processo de gestão de incidentes;

II. **DETECÇÃO E ANÁLISE (DETECTION AND ANALYSIS):** Fase que visa identificar a ocorrência de um incidente de segurança e entender sua natureza e impacto. Consiste no monitoramento contínuo do ambiente tecnológico da CMB; Utilização de ferramentas e técnicas de detecção para identificar incidentes; Coleta e análise dos dados relevantes para determinar a natureza, extensão e impacto do incidente; Classificação, priorização e notificação dos incidentes com base em seu impacto e urgência;

III. **CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO (CONTAINMENT, ERADICATION, AND RECOVERY):** Nesta etapa a equipe de resposta a incidentes deve determinar a estratégia de contenção mais adequada para impedir a propagação de um incidente e reduzir os danos; Coletar evidências que podem ser utilizadas para investigação forense ou processos judiciais; Identificar e neutralizar a origem do ataque e determinar quais etapas são necessárias para neutralizá-la; Erradicação completa das ameaças e recuperação dos sistemas afetados;

IV. **PÓS-INCIDENTE (POST-INCIDENT):** Fase final destinada para aprender com os incidentes ocorridos e melhorar os processos para tratamento futuro de novos incidentes. Deve ser conduzido uma revisão detalhada do incidente e da resposta, identificando o que funcionou bem e o que precisa ser melhorado; Documentar todos os aspectos do incidente, incluindo sua detecção, análise, contenção, erradicação, recuperação e lições aprendidas; Preparar relatórios detalhados para a gerência e outras partes

interessadas, conforme necessário; Identificar lacunas e a necessidade de capacitação da equipe de resposta a incidentes.

QUANTO AO SEU PROCEDIMENTO

3.4. A CONTRATADA deverá monitorar e analisar continuamente os eventos suspeitos com o objetivo de confirmar possíveis incidentes (eliminação de falsos positivos), considerando alertas gerados por soluções de segurança, log's de sistemas e de ativos tecnológicos, informações provenientes de fontes públicas e fontes de Threat Intelligence, além de informações fornecidas pela própria CMB. O seguinte conjunto de boas práticas deverá ser adotado para auxiliar nesta validação:

I. Traçar uma "baseline" padrão do ambiente, de forma a medir as características da atividade esperada (comportamento normal), visando que variações possam ser mais facilmente identificadas (comportamento anormal), devendo ter a capacidade de identificar ao menos os seguintes tipos de anomalias:
   a) Baseadas em Análise Estatística Comportamental (Statistical Behavioral Analysis);
   b) Baseadas em Análise de Tendências de Comportamento (Trend Behavior Analysis);
   c) Baseadas em limiares específicos (Thresholds);
   d) Baseadas em Aprendizado de Máquina (Machine Learning).

II. Conduzir caça a ameaças (threat hunting) buscando identificar atividades maliciosas que podem ter passado despercebidas. A caça às ameaças deverá ser conduzidas de forma proativa e orientada por hipóteses, utilizando técnicas, ferramentas e conhecimentos avançados de investigação para descobrir ativamente ameaças desconhecidas (Zero Day), avançadas (ATP), internas, atividades de hackers em estágio inicial ou outras atividades maliciosas que possam ter evitado a detecção pelas medidas de segurança convencionais;

III. Manter e usar uma base de conhecimento que deve incluir informações para consultas rápidas durante a análise dos incidentes. Esta base deve conter uma variedade de informações relacionadas ao ambiente da CMB, geradas pelas análises de incidentes ocorridas ao longo do tempo;

IV. Trabalhar em colaboração com equipes externas de CSIRT (Computer Security Incident Response Team) e a própria equipe da CMB para auxiliar na realização de investigações de ameaças, determinação da causa e natureza dos incidentes;

V. Participar ativamente de comunidades de segurança cibernética, fóruns online e grupos de pesquisa para trocar informações e colaborar na identificação e mitigação de ameaças.

3.5. Uma vez confirmado o incidente, a CONTRATADA deverá realizar uma “Triagem Básica do Incidente”, que consistirá na coleta de informações preliminares, sua categorização e priorização. Ao final, deverá ser gerado um “Relatório Preliminar do Incidente” contendo todas essas informações. Ao menos as seguintes informações preliminares do incidente, quando tecnicamente viável, devem ser coletadas e documentadas:

I. Quais ativos, redes, sistemas ou usuários foram afetados;

II. Quem ou o que originou o incidente;

III. Como o incidente ocorreu (Ex. quais ferramentas ou métodos de ataque usados, quais vulnerabilidades exploradas, etc.).

3.6. A CONTRATADA deverá comunicar a CMB sobre qualquer incidente identificado no ambiente, devendo ser encaminhado o “Relatório Preliminar do Incidente” elaborado durante a “Triagem Básica do Incidente”;

3.7. Os incidentes deverão ser categorizados de acordo com as informações preliminares obtidas, devendo atualizá-lo à medida que mais informações são coletadas e que a investigação se desenvolve. Segue abaixo tabela exemplificativa, não limitando-se a estas, de possíveis categorias que podem ser utilizadas;

CATEGORIA DO INCIDENTE	TIPO DE INCIDENTE
Conteúdo ou atividades abusivas	• Spam • Harassment • Pornography/Child Abuse/Violence • HR and Legal investigations • Malicious Insider

Comprometimento de conta	• Privileged account compromise • Unprivileged account compromise • Unauthorized Privilege Escalation • Application account compromise
Disponibilidade	• System Outage (malicious) • Data availability (malicious) • DoS/DDoS
Violação	• Unauthorized access to information • Unauthorized data modification • Data Exfiltration • Privacy Violation
Engenharia social	• Phishing • Vishing • Smishing • Business Email Compromise • Brand Spoofing • Rogue Wireless Access Point • IoT device impersonation • Website Takedowns
Coleta de informações	• Scanning • Sniffing • Social engineering (for information gathering pre-exploit)
Intrusão do sistema	• Exploiting known vulnerabilities • Login attempts • Point of Sales terminal intrusion • Network intrusion
Ativo perdido ou roubado	• Mobile Phone • Laptop computer • Media (USB drive etc) • IoT device
Malware e código malicioso	• Virus • Worm • Trojan • Spyware • Bot • Ransomware

Ataque a Website	• Website defacement • SQL injection • XSS

3.8. Os incidentes deverão ser priorizados de acordo com as informações preliminares obtidas, não devendo ser tratados jamais por ordem de chegada/identificação;

3.8.1. A tabela abaixo se propõe a prover critérios objetivos para orientar a CONTRATADA quanto aos níveis de "IMPACTO" (grau em que o serviço/dado foi impactado) e "URGÊNCIA" (Prioridade em que o incidente deve ser resolvido) para a correta atribuição de prioridade aos incidentes, onde "P1" indica a mais alta prioridade e "P5" a menor prioridade:

PRIORIZAÇÃO		**IMPACTO**		
		Alto	Médio	Baixo
URGÊNCIA	Alta	**P1**	**P2**	**P3**
	Média	**P2**	**P3**	**P4**
	Baixa	**P3**	**P4**	**P5**

- DESCRIÇÃO DO IMPACTO:
  - ✓ **Alto:** Não é mais possível fornecer serviços críticos a nenhum usuário e/ou informações confidenciais foram acessadas, exfiltradas ou criptografadas;
  - ✓ **Médio:** Não é mais possível fornecer serviços críticos a um subconjunto de usuários e/ou informações confidenciais foram corrompidas;
  - ✓ **Baixo:** É possível fornecer serviços a todos os usuários, mas com eficiência prejudicada e/ou informações não classificadas foram acessadas, exfiltradas ou corrompidas.
- DESCRIÇÃO DA URGÊNCIA:

- ✓ **Alta:** Incidente está em andamento e requer atenção imediata, a fim de interromper a sua continuidade;
- ✓ **Média:** Incidente não está em andamento, porém com risco iminente nova exploração;
- ✓ **Baixa:** Incidente não está em andamento e não representa risco iminente de exploração.

3.8.2. A priorização visa assegurar que recursos e esforços sejam direcionados inicialmente para incidentes que representam maior risco à segurança, permitindo uma resposta mais eficaz e tempestiva à possíveis intrusões.

3.9. Finalizada a "triagem básica", deverá ser iniciado o registro do incidente, mantendo atualizado o seu status e as evidências coletadas durante toda a investigação, permitindo que a CMB acompanhe desde o momento em que o incidente foi detectado até a sua resolução. Ao final do seu tratamento, ao menos as seguintes informações deverão constar no registro do incidente:

I. **Status Atual:** Indica o estágio do ciclo de vida do incidente (Ex. novo, em andamento, encaminhado, resolvido, etc.);
II. **Data e Hora:** Informação sobre a data e a hora da ocorrência do incidente;
III. **Categorização e priorização:** Informação sobre a categoria e nível de priorização do incidente;
IV. **Resumo:** Uma visão geral do incidente;
V. **Indicadores:** IoCs que foram usados para identificar o incidente;
VI. **Incidentes Relacionados:** Registros de incidentes que podem estar conectados ao atual;
VII. **Ações Tomadas:** Detalhamento das ações realizadas durante a investigação e resolução do incidente;
VIII. **Avaliações de Impacto:** Análise dos danos e consequências do incidente;
IX. **Contato:** Contatos realizados com indivíduos relevantes;
X. **Evidências Coletadas:** Detalhamento de todas as evidências reunidas durante a resposta;
XI. **Comentários:** Observações e insights dos membros da equipe de resposta a incidentes;
XII. **Próximos Passos:** Ações recomendadas após a resolução do incidente.

3.10. Os incidentes deverão passar por uma análise profunda, baseando-se no comportamento do ataque, identificando e evidenciando os principais vetores que levaram ao incidente e o seu real autor;

3.10.1. O aprofundamento da investigação dos incidentes consistirá em reunir todas as suas informações e evidências pertinentes, além de analisar mais detalhadamente os seus efeitos, extensão e impacto;

3.10.2. Quando cabível, deverá ser realizado a reconstrução do ataque em ambiente controlado, permitindo uma percepção mais realista do seu comportamento;

3.10.3. Todo o processo de análise e resultados obtidos deve ser documentado, incluindo os impactos observados, as vulnerabilidades exploradas, o método e a origem do ataque;

3.10.4. Deverá ser gerado e encaminhado à CMB “Relatório Completo do Incidente” detalhando todas as informações e evidências coletadas;

3.10.5. As evidências coletadas deverão visar não só a resolução do incidente, mas também viabilizar sua utilização para fins de processos judiciais, caso necessário. Um registro detalhado deve ser mantido para todas as evidências coletadas, incluindo o seguinte:

I. Informações de identificação (Ex. localização, número de série, número do modelo, nome do host, endereços de controle de acesso à mídia (MAC) e endereços IP);

II. Nome, cargo de cada indivíduo que coletou ou manipulou as evidências durante a investigação;

III. Data e hora (incluindo fuso horário) de cada ocorrência de manipulação de evidências;

IV. Lista de locais onde as evidências foram armazenadas.

3.10.6. Todas as evidências deverão ser devidamente documentadas e preservadas pelo período mínimo de **12 (doze) meses**, devendo ser recolhidas de acordo com procedimentos que cumpram todas as leis e regulamentos aplicáveis;

3.10.7. Sempre que as evidências forem transferidas de pessoa para pessoa, os formulários da cadeia de custódia devem detalhar a transferência e incluir a assinatura de cada parte;

3.10.8. Todos as evidências relativas ao incidente devem ser datadas e assinadas pelo responsável pelo tratamento do incidente;

3.10.9. Apenas pessoas autorizadas deverão ter acesso à base de dados de incidentes. As evidências devem ser criptografadas e protegidas de outras formas para que apenas pessoas autorizadas possam lê-las;

3.11. Incidentes atribuídos com prioridade máxima (P1) deverão ser tratados imediatamente pela CONTRATADA, antes mesmo do aprofundamento da sua investigação, visando tomar decisões rápidas e objetivas para interromper o incidente antes que cause impactos mais significativos ao ambiente, proporcionando tempo para o desenvolvimento de uma estratégia de remediação ou mitigação mais personalizada;

3.11.1. Uma vez realizada a contenção imediata do incidente de alta prioridade, caberá à CONTRATADA retorná-lo ao seu fluxo normal de análise, de forma a iniciar o aprofundamento detalhado da sua investigação

3.12. Deverá ser verificada a viabilidade da criação ou atualização de “playbooks” para a resposta automatizada de incidentes baseado nas informações coletadas na investigação;

3.13. De posse de todas as informações derivadas da análise do incidente, deverá ser realizada a sua devida contenção, o que poderá ocorrer com base nos procedimentos previamente definidos no **“Plano de Gerenciamento de Incidentes”** ou através do desenvolvimento um plano de contenção mais adequado, baseado nas especificidades observadas do incidente;

3.13.1. Para a contenção do incidente, independentemente do seu nível de prioridade, a CONTRATADA deverá atuar sempre dentro dos limites delineados por este Termo de Referência, carecendo previamente de uma análise quanto as ações necessárias e seu escopo de atuação;

3.13.2. Quando indispensável a atuação da CMB na contenção do incidente, a CONTRATADA deverá encaminhar documento denominado **“Plano de Contenção”**, o que deve incluir as ações já tomadas pela CONTRATADA e as instruções que detalhem as ações que devem ser executadas pela CMB. A atuação da CMB para contenção do incidente poderá ocorrer de forma autônoma ou mediante o consentimento à CONTRATADA para acesso temporário aos ativos/serviços tecnológicos internos da CMB;

3.13.3. A CONTRATADA deverá atuar proativamente na contenção dos incidentes, em conformidade com o seu limite de atuação, devendo comunicar a CMB sempre que qualquer ação de contenção for realizada no ambiente;

3.13.4. Caberá ainda à CONTRATADA, em conjunto com a CMB, analisar se as ações tomadas para conter o incidente produziram os resultados esperados, não só no sentido de averiguar se o incidente de fato foi contido, mas também para verificar se as ações, a depender do tipo de ataque envolvido, podem ter desencadeado danos adicionais inesperados.

3.14. Após a sua contenção, poderá ser necessária a erradicação do incidente e a recuperação dos serviços corporativos afetados, cabendo à CONTRATADA, em conjunto com a CMB, elaborar um do “Plano de Erradicação e Recuperação do Incidente”;

3.14.1. A erradicação do incidente terá como foco a eliminação dos componentes do ataque e a mitigação de todas as vulnerabilidades que foram exploradas, tal como:

I. limpeza completa e recriação de imagens dos discos rígidos do sistema afetado;

II. Atualizar e aplicar patches de segurança para corrigir vulnerabilidades em sistemas operacionais, aplicativos e dispositivos de rede;

III. Desativar serviços não utilizados (hardening);

IV. Remover todo o conteúdo malicioso dos sistemas afetados;

V. Utilizar ferramentas especializadas para detectar e remover malware;

VI. Substituir arquivos comprometidos por versões limpas;

VII. Reforçar a segurança através das soluções tecnológicas de segurança implementadas;

VIII. Desativação de contas de usuários violadas;

IX. Realizar simulações de ataque controlado.

3.14.2. A recuperação dos serviços afetados terá como foco a restauração da operação normal dos sistemas, tal como:

I. Definição de data e hora adequado para restauração do backup;

II. Restaurar o sistema operacional a partir de um ponto de restauração seguro antes da infecção;

III. Reconstrução de sistemas do zero;

IV. Realizar testes de funcionalidade e desempenho dos sistemas para assegurar que estão operando corretamente;

V. Monitorar e analisar o tráfego de rede para identificar padrões suspeitos que possam indicar a presença de ameaças remanescentes;

VI. Configurar alertas em sistemas de monitoramento para detectar qualquer atividade suspeita ou tentativas de reinfecção.

3.14.3. A CONTRATADA deverá auxiliar a CMB em todo o processo de erradicação do incidente e recuperação dos serviços afetados, acompanhamento do seu andamento e estando disponível para esclarecimento de eventuais dúvidas;

3.14.4. Caberá à CMB avaliar a necessidade de acionar o seu processo interno de gestão de mudanças para execução das ações necessárias para erradicação e recuperação dos incidentes.

3.15. Será de responsabilidade da CONTRATADA enviar, até o 5º (quinto) dia útil do mês subsequente, **relatório mensal** de acompanhamento dos incidentes (relatório de lições aprendidas), que deverá conter todas as informações importantes coletadas, descobertas e ações executas durante seu tratamento, além da proposição de melhorias ao Processo de Gestão de Incidentes;

3.15.1. O relatório deverá possuir uma descrição dos incidentes, como foram descobertos e quando foram relatados;

3.15.2. Deverá conter quaisquer descobertas sobre como o incidente ocorreu, incluindo uma análise de causa raiz;

3.15.3. Deverá conter um conjunto de dados objetivos e subjetivos relativos aos incidentes, que devem auxiliar na resposta das seguintes perguntas:

I. O que exatamente aconteceu e em que momentos?

II. Qual foi o desempenho da equipe e da gerência ao lidar com o incidente?

III. O procedimento documentado foi seguido e estava adequado?

IV. Existem áreas onde o treinamento pode ser considerado para melhoria do processo?

V. Que informações foram necessárias e não estavam disponíveis?

VI. Foram tomadas quaisquer medidas ou ações que possam ter inibido a recuperação?

VII. O que a equipe e a gerência fariam de diferente na próxima vez que ocorresse um incidente semelhante?

VIII. Como o compartilhamento de informações poderia ter sido melhorado?

IX. Que ações corretivas podem evitar incidentes semelhantes no futuro?

X. Que indicadores devem ser observados no futuro para detectar incidentes semelhantes?

XI. Os controles de segurança existentes foram suficientes e eficazes? Que ferramentas ou recursos adicionais são necessários para detectar, analisar e mitigar incidentes futuros?

XII. As ferramentas estão funcionando de acordo com as necessidades da organização?

XIII. Existem ataques novos e emergentes envolvidos nos incidentes?

XIV. Foi identificada o uso de Inteligência Artificial (IA) pelo invasor?

3.15.4. Deverá trazer recomendações que possam ser usadas para auxiliar no tratamento de incidentes futuros semelhantes;

3.15.5. Deverá seguir uma cronologia formal de eventos e ações tomadas, incluindo informações sobre a data/hora dos dados registrados no sistema eletrônico;

3.15.6. Deverá trazer recomendações para evolução e amadurecimento do Processo de Gestão de Incidentes.

3.16. A CONTRATADA deverá se **reunir mensalmente** com a CMB**,** até o 10º (décimo) dia útil do mês subsequente, para apresentar o relatório de lições apreendidas, os incidentes identificados e tratados no período, além de eventuais impactos e dificuldades observados;

3.16.1. Excepcionalmente, para incidentes de maior prioridade (P1), a CONTRATADA deverá se reunir com a CMB em **até 3 (três) dias úteis** após a conclusão do seu tratamento, não excluindo a necessidade da reunião mensal periódica;

3.16.2. Esta reunião será considerada a etapa final para o encerramento dos incidentes, tendo como principal objetivo o desenvolvimento dos processos e equipes envolvidas;

3.16.3. Caberá à CONTRATADA garantir que apenas as pessoas certas e necessárias estejam envolvidas na reunião;

3.16.4. Todas as reuniões deverão ser gravadas, cabendo à CONTRATADA documentar os principais pontos da reunião e realizar os esclarecimentos de dúvidas que possam surgir.

3.17. A CMB deverá aprovar quaisquer mudanças propostas para evolução e amadurecimento do processo, cabendo à CONTRATADA documentá-las e implementá-las dentro do prazo máximo de **até 15 (quinze) dias úteis**;

3.18. A modelagem do Processo de Gestão de Incidentes pode ser observada em **"Modelagem dos Processo" (APENSO I)** deste Termo de Referência.

QUANTO AOS SEUS INDICADORES-CHAVE (KPI'S)

DENOMINAÇÃO	DESCRIÇÃO
Quantitativo de ameaças detectadas	Número total de ameaças detectadas. Percentual (%): por tipo, severidade e origem.
Quantitativo de incidentes detectados	Número total de incidentes identificados. Percentual (%): por tipo e severidade.
Quantitativo de incidentes reincidentes	Número total de incidentes recorrentes. Percentual (%): por tipo e severidade.
Quantitativo de resposta aos incidentes	Número total de incidentes contidos ativamente pela equipe de resposta. Percentual (%): por tipo e origem.
Quantitativo de tentativas de ataque	Número total de tentativas de ataque identificadas. Percentual (%): por tipo e origem.
Quantitativo de falso positivo	Número total de incidentes e ameaças consideradas como falso positivo. Percentual (%): por tipo.
Quantitativo de falso negativo	Número total de incidentes e ameaças reais que não foram detectadas. Percentual (%): por tipo.
Tempo médio de detecção	Tempo médio entre a ocorrência de um incidente ou uma ameaça até a sua detecção. Percentual (%): por tipo e severidade.

Tempo médio de resposta	Tempo médio entre a detecção do incidente ou uma ameaça até a sua resposta. Percentual (%): por tipo e severidade.
Tempo médio de análise dos incidentes	Tempo médio de análise dos incidentes em cada fase do “Ciclo de Vida de Gestão de Incidentes” Percentual (%): por fase
Percentual de resolução	Porcentagem (%) de incidentes e ameaças tratadas em relação ao número total identificado (por tipo e severidade).
Percentual dos vetores de ataques	Percentual (%) dos principais vetores de ataques identificados (por tipo e severidade).

4. GESTÃO DE VULNERABILIDADES CIBERNÉTICAS

QUANTO A SUA DESCRIÇÃO

4.1. A CONTRATADA será responsável por monitorar e avaliar, de forma proativa e permanente, todo o ambiente tecnológico da CMB, visando detectar e corrigir vulnerabilidades de cibersegurança que possam ser exploradas por atores de ameaça, prevenindo possíveis impactos aos negócios da CMB;

4.2. Deverão ser empregadas atividades voltadas para identificação, priorização, documentação e correção/mitigação vulnerabilidades do parque tecnológico da CMB, além do monitoramento e classificação dos riscos relacionados à empresas terceiras e ativos da CMB expostos externamente, a fim de identificar brechas de segurança que possam comprometer a disponibilidade, integridade ou confidencialidade dos dados ou sistemas corporativos;

4.3. Para a execução adequada dessa atividade, deverá ser tomada como base as fases listadas abaixo, que juntas compõem o “Ciclo de Vida de Gestão de Vulnerabilidades” a ser executado pela CONTRATADA:

I. **AVALIAR (ASSESS):** Fase inicial no qual deverá ser realizada a identificação dos ativos, verificação das vulnerabilidades e elaboração de relatórios. Deve fornecer uma visão abrangente da postura de segurança da CMB e identificar os pontos fracos que requerem atenção;

II. **PRIORIZAR (PRIORITIZE):** Fase em que as vulnerabilidades deverão ser classificadas e ordenadas com base em sua gravidade, ou seja, visa

determinar a ordem em que as ações corretivas devem ser tomadas para mitigar os riscos de segurança;

III. **AGIR (ACT):** Fase em que respostas às vulnerabilidades deverão ser tomadas de acordo com as informações obtidas nas fases anteriores. Essa fase está intimamente ligada à execução das medidas necessárias para remediar, mitigar ou aceitar os riscos identificados;

IV. **REAVALIAR (REASSESS):** Etapa em que deverá ser assegurada a eficácia das ações tomadas durante a fase anterior. Fase crucial para garantir que o nível atual de risco permaneça em consonância com as expectativas;

V. **MELHORAR (IMPROVE):** Essa fase se concentrará em medir o desempenho do Processo de Gestão de Vulnerabilidades e identificar formas de melhorar continuamente sua maturidade e capacidade de gerenciar riscos adequadamente.

QUANTO A SEU PROCEDIMENTO

4.4. A CONTRATADA deverá realizar a identificação/descoberta dos ativos presentes no ambiente tecnológico da CMB e expostos na internet, permitindo uma visão clara e abrangente de toda a sua infraestrutura. Para isso, ao menos as seguintes ações devem ser realizadas:

I. **Inventário de ativos:** Levantamento completo de todos os ativos tecnológicos da CMB, através da utilização de recurso de descoberta automatizada e/ou manual;

II. **Mapeamento de dependências:** Identificar a interconexão entre os ativos e suas dependências, de forma a entender como as vulnerabilidades em um ativo podem impactar outros componentes do sistema e facilitar a gestão de riscos;

III. **Identificação de proprietários:** Para cada ativo, deverá ser atribuído um proprietário responsável (matriz de responsabilidade);

IV. **Atualização contínua:** O inventário de ativos deverá ser revisado e atualizado regularmente para garantir que novos ativos sejam adicionados e que ativos desativados sejam removidos.

4.5. Deverá realizar a verificação das vulnerabilidades presentes no ambiente tecnológico da CMB, cabendo sua validação para garantir que sejam precisas, relevantes, legítimas e que foram compreendidas corretamente, visando a

eliminação possíveis falsos positivos antes das ações de remediação/mitigação cabíveis;

4.5.1. A verificação deverá ocorrer de forma contínua, devendo ser determinado a frequência e o período no qual serão executadas as varreduras no ambiente de acordo com a criticidade dos ativos, o que deverá constar no **"Plano de Gerenciamento de Vulnerabilidades"**;

4.5.2. A verificação de vulnerabilidades do ambiente deverá ocorrer tanto de forma passiva (através de varreduras que demonstrem a utilização de sistemas/serviços/softwares com versões vulneráveis, fora de conformidade ou com falhas de configuração), bem como de forma ativa (através da simulação de cenários controlados de ataques reais);

4.5.3. As informações coletadas, além de servir de guia para o processo de correção e mitigação das vulnerabilidades, também deverão ser utilizadas para fornecer contexto de análise e investigação para tratamento de incidentes de cibersegurança.

4.6. Classificar e ordenar as vulnerabilidades e falhas identificadas de acordo com o seu nível de gravidade, o que deverá ocorrer com base na combinação dos seguintes componentes:

I. **Risco inerente à vulnerabilidade:** Classificação atribuída através do Sistema de Pontuação de Vulnerabilidade Comum (Common Vulnerability Scoring System - CVSS);

II. **Risco inerente ao ativo:** Classificação atribuída com base na especificidade do ativo, tais como: (A) Classificação dos dados mantidos no ativo (Ex. dados protegidos por regulamentação), (B) riscos de arquitetura (Ex. ativos externos), (C) controles de compensação ativos (Ex. antimalware, IPS, etc.), entre outros;

III. **Risco de Inteligência de Ameaça (Threat Intel):** Classificação atribuída com base no contexto de ameaças atual, tais como: (A) vulnerabilidade é relatada como explorável no mundo real, (B) vulnerabilidade está em um software, sistema ou serviço amplamente utilizado, (C) um exploit está publicamente conhecido e/ou está disponível em bancos de dados online, (D) tentativas de exploração foram detectadas em uma organização ou indústria semelhante, entre outros;

IV. **Risco inerente a simulação de ataque:** priorizar esforços de correção utilizando uma abordagem proativa de avaliação de segurança, tomando

como base os resultados obtidos de ferramenta especializada de simulação de ataques cibernéticos do mundo real.

4.7. Uma vez realizada a identificação dos ativos, suas vulnerabilidades e feita sua classificação, deverá ser emitido um "Relatório de Correção das Vulnerabilidades" apontado todas as informações coletadas para a devida análise da CMB, incluindo sugestões de medidas de "remediação" e/ou "mitigação" cabíveis, além dos possíveis impactos que essas ações podem causar no ambiente;

4.7.1. Entende-se "remediação" como a correção imediata das vulnerabilidades. A ação de remediar envolve implementar pacotes de correções necessárias para eliminar totalmente as vulnerabilidades e tornar o ambiente mais seguro;

4.7.2. Entende-se "mitigação" como medidas adotadas para reduzir os riscos associados às vulnerabilidades, ou seja, medidas que minimizam a exploração de uma vulnerabilidade e seus possíveis efeitos prejudiciais, especialmente quando não há correções disponíveis ou quando a implementação imediata não é possível;

4.8. A CONTRATADA, em regra, não poderá atuar de forma autônoma na "remediação" ou "mitigação" das vulnerabilidades identificadas, devendo qualquer mudança no ambiente passar por previa autorização da CMB;

4.8.1. Para o caso de "remediação" das vulnerabilidades, admite-se a utilização de uma ou mais das seguintes formas:

I. **Automatizada:** Aplicação automática das correções em determinados ativos sem dependência de ação manual do administrador;

II. **Semiautomatizada:** Aplicação automática das correções em determinados ativos com dependência de ação manual do administrador;

III. **Manualmente:** Necessidade de acesso direto ao ativo para aplicação manual da correção ou para resolução de problemas que geraram falha no processo de correção automatizada ou semiautomatizada.

4.8.2. Para o caso de "mitigação" das vulnerabilidades, caberá a CONTRATADA sugerir medidas baseadas nas melhores práticas de segurança e apoiar a CMB na implementação destas medidas.

4.9. Após aprovação da CMB, as correções deverão ser aplicadas primeiramente em um conjunto limitado de ativos, a fim de que sejam previamente homologadas antes da sua aplicação no ambiente de produção;

4.9.1. A lista de ativos voltados para homologação das correções será definida previamente pela CMB. A CONTRATADA deverá manter essa lista de ativos atualizada conforme indicado pela CMB;

4.9.2. A aplicação das correções em todo o ambiente da CMB só poderá ocorrer após previamente homologadas.

4.10. A CONTRATADA deverá auxiliar a CMB na identificação todos os problemas/falhas ocasionados pelas correções aplicadas (direta ou indiretamente), devendo gerar “Relatório de problemas/falhas” com todas as informações coletadas e possíveis alternativas para correção.

4.10.1. Caberá à CONTRATADA avaliar a necessidade do acionamento de terceiros (Ex. fabricante) para auxiliar no processo de identificação problemas/falhas e alternativas para correção, devendo coordenar todas as interações que julgar necessárias;

4.10.2. Uma vez mapeados os problemas/falhas e traçadas todas as alternativas cabíveis para sua correção, deverá ser avaliado a viabilidade técnica da sua implementação no ambiente;

4.10.3. Caso a correção dos problemas/falhas mostre-se tecnicamente inviável, a CONTRATADA deverá elaborar “Relatório de Inviabilidade de Correção” contendo todos os motivos da inviabilidade. Além disso, a CONTRATADA será responsável por auxiliar a CMB no processo de rollback dos ativos afetados;

4.10.4. Sendo tecnicamente viável a correção dos problemas/falhas, a CONTRATADA deverá auxiliar a CMB na sua correta implementação.

4.11. A CONTRATADA só poderá aplicar as correções no ambiente de produção após explicita autorização da CMB, que deliberará quanto a necessidade de acionar o seu processo interno de gestão de mudanças;

4.12. A CMB poderá decidir também por não aplicar nenhuma medida de “remediação” ou “mitigação” para uma vulnerabilidade identificada, o que será considerado como “aceitação ao risco”;

4.12.1. Caberá à CONTRATADA documentar todas as decisões de “aceitação ao risco” tomadas pela CMB, devendo manter registrado ao menos as seguintes informações:

I. Nome da pessoa que tomou a decisão;
II. O motivo da aceitação do risco;
III. Prazo de expiração da decisão (não podendo ultrapassar o máximo de 6 (seis) meses).

4.12.2. Atingido o prazo determinado de expiração da decisão, a CONTRATADA deverá cobrar novamente a resolução do problema, devendo manter os registros atualizados das novas decisões manifestadas pela CMB;

4.12.3. Excepcionalmente, uma decisão de “aceitação ao risco” poderá não ter um prazo de expiração definido, o que deverá ocorrer apenas nos casos em que for determinado que os custos, esforços ou possíveis impactos de implementar medidas de “correção” ou “mitigação” excedem os riscos associados à própria vulnerabilidade.

4.13. Após da correção das vulnerabilidades, a CONTRATADA deverá realizar a avaliação dos resultados das medidas de “remediação” ou “mitigação” aplicadas, o que deverá ocorrer por meio de uma nova avaliação das vulnerabilidades (ativa e passiva);

4.13.1. Realizar a simulação de cenários controlados de ataques reais para identificar possíveis lacunas de segurança, proporcionando uma compreensão mais fidedigna da resiliência do ambiente, atuando como um processo complementar à verificação passiva de vulnerabilidades;

4.13.2. Uma vez realizada a revalidação, deverá ser emitido “Relatório de Reavaliação de Vulnerabilidades” apontando todos os resultados obtidos, incluindo novas sugestões de medidas de “remediação” e “mitigação” cabíveis, caso as medidas de correção iniciais não tenham surtido o efeito esperado;

4.13.3. Uma nova avaliação quanto ao acionamento processo interno de gestão de mudanças da CMB será necessária caso ainda sejam identificadas a implementação de novas medidas de “remediação” e “mitigação”.

4.14. Será de responsabilidade da CONTRATADA enviar, até o 5º (quinto) dia útil do mês subsequente, **relatório mensal** de acompanhamento das vulnerabilidades, que deverá conter todas as informações importantes coletadas, descobertas e ações executas durante sua correção, além de propor melhorias ao Processo de Gestão de Vulnerabilidades;

4.14.1. O relatório deverá possuir uma descrição das vulnerabilidades, como foram descobertas e quando foram relatadas;

4.14.2. Deverá conter quaisquer descobertas sobre como a vulnerabilidade ocorreu, incluindo uma análise de causa raiz;

4.14.3. Deverá conter um conjunto de dados objetivos e subjetivos relativos as vulnerabilidades, que devem auxiliar na resposta das seguintes perguntas:

I. O que exatamente aconteceu e em que momentos?

II. Qual foi o desempenho da equipe e da gerência ao lidar com as vulnerabilidades?

III. Os procedimentos documentados foram seguidos e estavam adequados?

IV. Existem áreas onde o treinamento pode ser considerado para melhoria do processo?

V. Que informações foram necessárias e não estavam disponíveis?

VI. Foram tomadas quaisquer medidas ou ações que possam ter inibido o processo?

VII. O que a equipe e a gerência fariam de diferente na próxima vez?

VIII. Como o compartilhamento de informações poderia ter sido melhorado?

IX. Que ações corretivas podem evitar vulnerabilidades semelhantes no futuro?

X. Que indicadores devem ser observados no futuro para detectar vulnerabilidades semelhantes?

XI. Que ferramentas ou recursos adicionais são necessários para detectar, analisar e mitigar vulnerabilidades futuras?

XII. As ferramentas estão funcionando de acordo com as necessidades?

XIII. Existiram vulnerabilidades novas e emergentes envolvidas?

4.14.4. Deverá trazer recomendações que possam ser usadas para auxiliar no tratamento de vulnerabilidades futuras semelhantes;

4.14.5. Deverá seguir uma cronologia formal de eventos e ações tomadas, incluindo informações de data/hora do ocorrido;

4.14.6. Deverá trazer recomendações para evolução e amadurecimento do Processo de Gestão de Vulnerabilidades.

4.15. A CONTRATADA deverá se **reunir mensalmente** com a CMB, até o 10º (décimo) dia útil do mês subsequente, para apresentar o relatório de acompanhamento das vulnerabilidades, as vulnerabilidades identificadas e corrigidas no período, além de eventuais impactos e dificuldades observados;

4.15.1. Esta reunião será considerada a etapa final para o encerramento das vulnerabilidades, tendo como principal objetivo o desenvolvimento dos processos e das equipes envolvidas;

4.15.2. Caberá à CONTRATADA garantir que apenas as pessoas certas e necessárias estejam envolvidas na reunião;

4.15.3. Todas as reuniões deverão ser gravadas, cabendo à CONTRATADA documentar os principais pontos da reunião e realizar os esclarecimentos de dúvidas que possam surgir.

4.16. A CMB deverá aprovar quaisquer mudanças propostas para evolução e amadurecimento do processo, cabendo à CONTRATADA documentá-las e implementá-las dentro do prazo máximo de **até 15 (quinze) dias úteis;**

4.17. A modelagem do Processo de Gestão de Vulnerabilidades pode ser observada em **"Modelagem dos Processo" (APENSO I)** deste Termo de Referência.

QUANTO AOS SEUS INDICADORES-CHAVE (KPI'S)

DENOMINAÇÃO	DESCRIÇÃO
Quantitativo de vulnerabilidades	Número total de vulnerabilidades identificadas. Percentual (%): por tipo e severidade.
Quantitativo de simulações	Número total de simulações de ataque realizadas. Percentual (%): por tipo.
Quantitativo de Vulnerabilidades reincidentes	Número total de vulnerabilidades recorrentes. Percentual (%): por tipo e severidade.
Quantitativo de vulnerabilidades corrigidas	Número total de vulnerabilidades corrigidas. Percentual (%): por tipo e severidade.
Quantitativo de correções pendentes	Número total de vulnerabilidades que não puderam ser corrigidas devida a pendencias. Percentual (%): por tipo e severidade.
Quantitativo de falso positivo	Número total de vulnerabilidades consideradas como falso positivo. Percentual (%): por tipo.

Quantitativo de falso negativo	Número total de vulnerabilidades reais que não foram detectadas pelo sistema. Percentual (%): por tipo.
Tempo médio para correções	Tempo médio entre a identificação de uma vulnerabilidade e sua correção efetiva. Percentual (%): por tipo e severidade.
Percentual de resolução de vulnerabilidades	Porcentagem (%) de vulnerabilidades tratadas em relação ao número total identificado (por tipo e severidade).
Percentual de risco	Percentual (%) de risco geral do ambiente, considerando todas as vulnerabilidades ativas e seu grau de severidade.
Percentual de Correções	Porcentagem (%) de vulnerabilidades corrigidas em relação ao número total identificado (por tipo e severidade).
Percentual de Sucesso da Simulação	Percentual (%) de simulações de ataque que conseguiram explorar vulnerabilidades ou comprometer sistemas (por tipo e severidade).

5. SOLUÇÕES TECNOLÓGICAS DE CIBERSEGURANÇA

5.1. INCIDENT MANAGEMENT PLATFORM

5.1.1. A solução tecnológica ofertada, ou o conjunto de soluções integradas, deverá proporcionar monitoramento, detecção e resposta de incidentes cibernéticos, oferecendo uma visão unificada e em tempo real dos eventos de cibersegurança. Para tanto, a solução deverá contemplar, no mínimo, as seguintes funcionalidades:

I. Security Information and Event Management (SIEM) com User and Entity Behavior Analytics (UEBA) integrado;

II. Security Orchestration, Automation and Response (SOAR) ou similar (Ex. Workflow automation);

III. Network Detection and Response (NDR) com Intrusion Detection System (IDS) e sandbox integrados.

5.1.2. Deverá coletar logs, visando realizar o seu correlacionamento para identificação de anomalias e incidentes de cibersegurança, para ao menos as seguintes fontes de dados:

I. Servidores Windows e Linux (físicos e virtuais);

II. Desktops Windows e Linux (físicos e virtuais);

III. Plataformas Hypervisors (mínimo VMWare);

IV. Switches, Roteadores e Access Points;

V. Soluções do Microsoft 365 (M365 E3 + M365 E5 Compliance com 1900 usuários ativos);

VI. Todas as soluções tecnológicas ofertadas nesta contratação.

5.1.3. Deverá ter a capacidade de receber log's provenientes de ao menos **2.500 (dois mil e quinhentos) fontes de dados (ativos) simultâneas**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais fontes de dados conforme sua preferência, desde que respeitado o limite estabelecido;

5.1.3.1. Deve permitir o recebimento ilimitado de eventos dessas fontes de dados, tendo inclusive a capacidade de eventualmente operar acima do estimado inicialmente sem perder qualquer funcionalidade/capacidade.

5.1.3.2. No caso da solução não puder ser dimensionada com base no número de ativos, será de responsabilidade da CONTRATADA, com base nas informações disponibilizadas na tabela abaixo, realizar o cálculo adequado para estimar o volume de tráfego ou eventos que deverão ser disponibilizados para a CMB. No entanto, a solução obrigatoriamente deverá suportar o envio de log's para o quantitativo mínimo de ativos simultâneos indicado;

FONTES DE DADOS	QUANTIDADE
Servidores Windows	200
Servidores Linux	210
Hypervisors	20
Workstation	1500
Servidores de Banco de Dados	40
Switches, Roteadores e Access Points	450
Serviço E-mail	5
Serviço Web	50

Soluções do Microsoft 365 (M365 E3 + M365 E5 Compliance)	APENSO H
Soluções tecnológicas ofertadas nesta contratação	Em linha com os quantitativos solicitados neste documento

5.1.4. Deverá permitir a criação de ao menos **10 (dez) workflows/playbooks** para automatização de processos, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais workflows/playbooks conforme sua preferência, desde que respeitado o limite estabelecido;

5.1.5. Deverá ser dotada de console de administração centralizada, contemplando uma interface gráfica (Graphical User Interface - GUI) acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.);

5.1.6. Deverá fazer uso de protocolos seguros para comunicação criptografada entre os diferentes componentes da solução, assim como para o acesso à sua console de administração;

5.1.7. Deverá permitir autenticação Single Sign-On (SSO) integrada com os serviços do Active Directory Domain Services (AD DS) ou com o Microsoft Entra ID, o que poderá ocorrer através de um ou mais protocolos padrão de mercado, tais como: RADIUS, LDAP, SAML, OAuth, Kerberos, etc;

5.1.8. Deverá permitir a habilitação de autenticação por multifator (Multi-Factor Authentication - MFA) de terceiros ou do próprio fabricante para gerenciamento da solução;

5.1.9. Deverá permitir que usuários recebam permissões específicas com base em suas funções (Role-Based Access Control - RBAC);

5.1.10. Deverá gerar e manter o histórico completo de trilhas de auditoria que permita o rastreamento dos acessos executados pelos usuários (logs);

5.1.11. Não poderá apresentar limitação quanto ao número de acessos simultâneas autorizados a administrar a solução, desde que devidamente licenciados;

5.1.12. O fabricante da solução ofertada deve contar com rede de inteligência de ameaças (Threat Intelligence) para aprimoramento dos seus controles de segurança;

5.1.13. A CONTRATADA deverá fornecer todos os componentes necessários ao funcionamento da solução ofertada, conforme a arquitetura e condições mínimas estabelecidas neste documento;

5.1.13.1. A ação de **"análise do tráfego de rede (Sensor NDR)"** deverá ser executada exclusivamente por meio de "**Appliances Físicos"**, fornecidos e instalados nas dependências da CMB (on-premise), observadas as melhores práticas recomendadas pelo fabricante;

5.1.13.2. Para a ação de **"coleta e encaminhamento de logs (Collectors)"**, a CONTRATADA poderá utilizar os próprios "**Appliances Físicos"** ofertados ou, alternativamente, "**Appliances Virtuais"**, desde que observadas as seguintes condições mínimas:

I. Deverão ser instalados no ambiente de virtualização da CMB, sendo obrigatoriamente compatíveis com o hypervisor VMware;

II. Caso seja necessária a instalação de serviço complementar, este deverá ser compatível com sistemas operacionais Linux ou Windows, em servidor a ser fornecido e instalado pela própria CMB, cabendo à CONTRATADA fornecer todas as orientações necessárias para sua correta instalação, configuração e operação;

III. Quando utilizado sistema operacional Windows, a CMB disponibilizará apenas as licenças Windows Server Datacenter e respectivas CAL (Client Access License), cabendo à CONTRATADA fornecer todas as demais licenças eventualmente necessárias ao funcionamento da solução;

IV. Deverão ser instalados em rede definida pela CMB, atrás do seu firewall, observadas as recomendações do fabricante;

V. A CMB será responsável pela execução dos procedimentos de backup e recuperação dos Sensores Virtuais em caso de indisponibilidade, cabendo à CONTRATADA prestar todo o suporte necessário para a restauração do serviço;

VI. Deverão ser fornecidos em arquitetura de alta disponibilidade (High Availability – HA), observando os mesmos quantitativos exigidos para os "Appliances Físicos", de forma a assegurar a continuidade da coleta e encaminhamento de logs durante manutenções ou indisponibilidades do servidor hospedeiro.

5.1.13.3. Os **"Appliances Físicos"** deverão ser ofertados em diferentes tipos, observando-se que todos os requisitos e quantitativos especificados

deverão ser atendidos individualmente por cada equipamento, não sendo admitida a soma das capacidades dos equipamentos integrantes de um mesmo cluster para comprovação do atendimento. Os “Appliances Físicos” deverão conter, no mínimo, as seguintes especificações:

APPLIANCE FÍSICO – TIPO I	
QUANTIDADE: 2 (duas) unidades	
LOCALIDADE: Unidade Santa Cruz	
ATRIBUTO	**ESPECIFICAÇÃO**
Throughput	4 Gbps
Interfaces de Monitoramento	2x 1 Gbps cobre RJ45 (duas portas de um gigabit por segundo padrão RJ45) 2x 10 Gbps fiber singlemode LC (duas portas de dez gigabits por segundo para fibra monomodo padrão LC)
Interfaces de Gerenciamento	1x 1 Gbps cobre RJ45 (uma porta de um gigabit por segundo padrão RJ45)
Armazenamento	450 GB
Fonte de Energia	2x fontes 100-240V

APPLIANCE FÍSICO – TIPO II	
QUANTIDADE: 1 (uma) unidade	
LOCALIDADE: Unidade Flamengo	
ATRIBUTO	**ESPECIFICAÇÃO**
Throughput	1 Gbps
Interfaces de Monitoramento	3x 1 Gbps cobre RJ45 (três portas de um gigabit por segundo padrão RJ45)
Interfaces de Gerenciamento	1x 1 Gbps cobre RJ45 (uma porta de um gigabit por segundo padrão RJ45)
Armazenamento	128 GB
Fonte de Energia	1x fonte 100-240V

5.1.13.4. Os **“Appliances Físicos”** deverão ser fornecidos com kit de instalação compatível com rack padrão de 19" (dezenove polegadas) e vir acompanhados, quando necessário, de todos os transceivers compatíveis, em quantidade suficiente para atender o quantitativo de interfaces requisitadas;

5.1.13.5. Os appliances destinados à ação de **“análise do tráfego de rede (Sensor NDR)”** deverão suportar o monitoramento de tráfego proveniente de Port Mirroring (Switch Port Analyzer – SPAN) configurado em switches existentes na infraestrutura da CMB, bem como de Network TAPs (físicos ou virtuais) e Network Packet Brokers (NPB) compatíveis com a solução ofertada;

5.1.13.6. Os appliances destinados à ação de **“coleta e encaminhamento de logs (Collectors)”** deverão permitir a coleta de logs dos ativos tecnológicos da CMB através do padrão SYSLOG ou similar, a ingestão de logs protegidos por TLS utilizando certificados digitais válidos ou autoassinados, além da compressão dos registros e a aplicação de filtros antes do seu envio à plataforma de gestão de incidentes;

5.1.13.7. Todos os appliances ofertados (físicos e virtuais) deverão disponibilizar interface de gerenciamento por linha de comandos (Command Line Interface – CLI), além de possuir mecanismo de provisionamento que permita, após a aplicação de configurações básicas, conectar-se automaticamente à console de gerenciamento da solução, ficando a efetiva autorização de ingresso condicionada à aprovação do administrador;

5.1.13.8. A console de administração deverá permitir a atualização remota do software e/ou firmware de todos os dispositivos ofertados (físicos e virtuais), além do monitoramento do seu estado operacional (online/offline).

5.1.14. Os logs dos servidores e desktops da CMB poderão ser coletados por meio do uso de “agente”, fornecido pela CONTRATADA, compatíveis minimamente com sistemas operacionais Windows e Linux;

5.1.14.1. O “agente” instalado nas estações da CMB deve causar o mínimo impacto possível no consumo de recursos de hardware da estação,

assegurando que o desempenho geral do sistema não seja comprometido;

5.1.14.2. O “agente” deverá ter a capacidade de encaminhar os logs coletados para o appliances fornecidos (físicos ou virtuais).

5.1.15. A solução deverá ter a capacidade de realizar o inventário dos ativos identificados na rede, por endereços IP e o nível de risco, sem a necessidade de executar varreduras de rede para este fim;

5.1.16. Deverá correlacionar as vulnerabilidades relatadas por ferramentas de terceiros, com assinaturas de ataque identificadas e exibi-las em um painel de controle a partir dos quais os relatórios são gerados;

5.1.17. Deverá permitir a auditoria sobre o status das ações tomadas ou pendentes dentro do sistema;

5.1.18. Deverá possuir ao menos 100 (cem) conectores nativos (API) para integração facilitada com soluções de fabricantes diversos no mercado;

5.1.19. Deverá representar todos os dados brutos ingeridos em informações estruturadas e legíveis, através do enriquecendo, centralização e organização das informações de ameaças de segurança para uma análise mais ágil e eficiente;

5.1.20. Deverá realizar triagem automática de alertas/eventos, eliminando falsos positivos, alertas duplicados ou irrelevantes, devendo listá-los em uma visão geral e unificada. Deverá ainda permitir, a partir desta lista, o acesso aos detalhes dos alertas/eventos, possibilitando a visualização, no mínimo, das seguintes informações:

I. Nome do tipo de alerta/evento, acompanhado de link com maiores informações sobre o tipo de alerta;
II. Descrição mais detalhada do tipo de alerta/evento;
III. Data e a hora em que o alerta/evento ocorreu;
IV. Táticas e técnicas do Cyber Kill Chain utilizadas;
V. Pontuação de risco do alerta/evento;
VI. Status do alerta/evento (novo, em investigação, encerrado, etc.);
VII. Sensor que coletou os dados do alerta/evento;
VIII. Todos os usuários associados ao alerta/evento;
IX. Endereços IP de origem e destino e sua geolocalização.

5.1.21. Deverá permitir que sejam realizadas ações referentes aos alertas/eventos descobertos, devendo guardar todo o histórico de ações realizadas. Tais ações devem cobrir ao menos:

I. Criar filtros para ignorar alertas/eventos específicos;
II. Adicionar tags customizadas;
III. Adicionar comentários;
IV. Enviar e-mail de notificação;
V. Criar política para bloquear os IPs envolvidos;
VI. Desativar o usuário envolvido;
VII. executar um script personalizado.

5.1.22. Deverá associar automaticamente vários alertas de segurança individuais a um único “caso unificado”, proporcionando uma visão contextualizada e priorizada para investigação. Entende-se como “caso unificado” um conjunto de múltiplos alertas correlacionados que constituem um potencial ataque de segurança e classificado por uma pontuação atualizada dinamicamente, indicando a sua gravidade para resolução aprimorada;

5.1.23. Deverá permitir a criação de casos unificados manualmente, a partir de qualquer alerta existe no sistema;

5.1.24. Deverá permitir a atribuição dos casos a um profissional específico para tratamento, proporcionando a visibilidade da sua identificação, as ações executadas;

5.1.25. Deverá identificar anomalias nos comportamentos dos usuários, utilizando técnicas de User and Entity Behavior Analytics (UEBA) para traçar automaticamente uma baseline comportamental, devendo identificar ao menos os seguintes casos atípicos de uso:

I. Horário do acesso;
II. Volume de conexões;
III. Volume de transferências de dados;
IV. Localização geográfica;
V. Acesso por endereço IP incomum;
VI. Acesso incomum a dados;
VII. Criação e uso de processos pelo usuário;
VIII. Mudança na postura de risco do usuário.

5.1.26. Deverá fazer uso de Inteligência Artificial (IA) para aplicar técnicas de Machine Learning (ML) ou outros métodos analíticos que auxiliem no

processo de correlacionamento de eventos, geração e agrupando alertas, atividades suspeitas e incidentes de segurança;

5.1.27. Deverá possuir ferramentas nativa que auxiliem na investigação e busca por ameaças (threat hunter), com o objetivo de identificar ameaças ocultas;

5.1.28. Deverá possuir base de conhecimento de métricas, indicadores de intrusão ou comprometimento atualizadas periodicamente de acordo com a mudança do cenário de ameaças e surgimento de novas técnicas ou padrão de ataque;

5.1.29. Deverá fornecer ao menos uma linha do tempo, objetos associados, indicadores de métricas de Mean Time To Detect (MTTD) e Mean Time To Repair (MTTR) associados aos incidentes identificados;

5.1.30. Deverá priorizar os riscos baseado no contexto de ameaça e de criticidade dos ativos;

5.1.31. Deverá apresentar a localização e as informações das ameaças identificadas, tentativas de infiltração e risco, de acordo com as fases da Cadeia de Ataque (Cyber Kill Chain) e MITRE ATT&CK;

5.1.32. Deverá normalizar e contextualizar automaticamente os dados coletados com base em: inteligência de ameaças, Machine Learning, informações do usuário, informações dos ativos e geolocalização;

5.1.33. Deverá gerar diagramas de conexões mostrando como as ameaças estão associadas e se movem no ambiente;

5.1.34. Deverá realizar análise retrospectiva com base nos dados ingeridos e armazenados (base histórica), apoiando uma análise forense;

5.1.35. Deverá possuir regras de correlacionamento nativas, com contínua atualização automática pelo fabricante, além de permitir a criação de regras customizadas;

5.1.36. Deverá identificar protocolo pelo conteúdo das sessões, independente da porta utilizada de comunicação, permitindo a criação de interpretadores (parsers) para protocolos e aplicações proprietárias/não conhecidas OU permitir que a criação dos parsers possam ser requisitados ao fabricante da solução;

5.1.37. Deverá permitir a exportação dos logs coletados no formato texto JSON;

5.1.38. Deverá ter a capacidade de exportar e importar arquivos no formato packet capture (PCAP) ou CSV ou JSON;

5.1.39. Deverá permitir a geração de hash (MD5 e SHA1) para verificação de integridade dos arquivos extraídos a partir da captura do tráfego;

5.1.40. Deverá permitir a customização de “playbooks” para automatização de tarefas, além possuir “playbooks” pré-definidos nativamente na solução, possibilitando ao menos as seguintes ações:

I. Envio automático de alerta(s);
II. Criar políticas na solução de NGFW da CMB (APENSO H);
III. Desabilitar a conta de usuários específicos;
IV. Executar scripts personalizados;
V. Agendamento do intervalo de execução, além de permitir a execução independentemente do agendamento (sob demanda).

5.1.41. Deverá possuir "alertas" pré-definidos nativamente na solução, além de permitir a customização de novos:

5.1.42. Deverá permitir a criação e customização de dashboards e relatórios, além de viabilizar buscas interativas de informações pelo sistema;

5.1.43. Quanto ao período de retenção dos logs armazenados pela plataforma de gestão de incidentes, abrangendo tanto aqueles provenientes das diversas fontes de dados monitoradas (ativos) quanto os gerados pela própria plataforma, deverá ser adotada a seguinte política:

I. Armazenar localmente, **pelo período de 30 (trinta) dias**, os logs não tratados (raw logs) no “sensor físico” ou “sensor virtual” disponibilizado, garantindo a possibilidade de redirecionamento desses registros a um servidor syslog indicado pela CMB;
II. Armazenar, **pelo período de 90 (noventa) dias**, os log’s tratados (processed log’s) em ambiente de “hot storage”, garantindo sua plena disponibilidade para consulta, acesso imediato, análise, correlação e emissão de relatórios em tempo real;
III. Após o período de 90 (noventa) dias de retenção em “hot storage”, os logs tratados deverão ser automaticamente transferidos, de forma transparente e sem necessidade de intervenção manual, para ambiente de “cold storage”, onde deverão permanecer disponíveis para consultas e recuperação pelo **período mínimo de 5 (cinco) anos**. Uma vez feita a solicitação para restauração dos dados, estes devem começar a ser disponibilizados para a CMB em **até 24 (vinte a quatro) horas**. Os dados deverão estar protegidos por criptografia

durante a transferência e em repouso, observando-se as melhores práticas de cibersegurança.

5.1.44. A funcionalidade de Network Detection and Response (NDR) deverá analisar o tráfego TCP/UDP na rede da CMB para detectar comportamentos anômalos e possíveis ameaças, gerando eventos de alerta de acordo com o tipo de tráfego;

5.1.44.1. Deve realizar o aprendizado do ambiente de rede e a inspeção do tráfego, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede;

5.1.44.2. Deve identificar ameaças através do monitoramento proativo do tráfego de rede da CMB direcionado à solução, contemplando ao menos:

I. Utilização da largura de banda;
II. Tentativas de penetração e varreduras de IPs e portas;
III. Autenticações recusadas ou com falhas;
IV. Ataques bem-sucedidos de autenticação de força bruta;
V. Presença de tráfego malicioso, como ramsomware, movimentação lateral, crypojacking, mimekatz, etc;
VI. Análise de arquivos benignos e maliciosos e suas respectivas categorias;
VII. Ataques de negação de serviço;
VIII. Conexões de comando e controle presentes, internamente ou de/para a Internet;
IX. Dispositivos que representam o maior risco;
X. Tempos de resposta, tráfego de entrada e saída (inbytes/outbytes);
XI. Aplicações que consomem mais recursos de rede;
XII. Análise de DNS (tempos de resposta, comunicação, time-out, erros e desempenho);
XIII. Identificação das conexões e seu risco associado;
XIV. Identificação de aplicações da Camada 7;
XV. Principais eventos críticos de segurança.

5.1.44.3. Deve detectar padrões de ataques, através do emprego de um Intrusion Detection System (IDS), usando uma combinação de aprendizado de máquina supervisionado e não supervisionado,

heurística, assinaturas de ataque conhecidas e análise de malware de dia zero;

5.1.44.4. Deve contar com recurso de sandbox para análise de malwares em arquivos considerados suspeitos ou desconhecidos, devendo prevenir ataques (incluindo zero day) que tenham o objetivo de realizar atividades maliciosas, possuindo inclusive um mecanismo de pontuação de risco.

5.1.45. Todo o conjunto de funcionalidades exigidas para a solução tecnológica ofertada deverá operar de forma integrada e interoperável, sem prejuízo da flexibilidade prevista nos itens 1.34, 1.35 e 1.36.

5.2. NETWORK PACKET BROKER (NPB)

5.2.1. Deverá ser fornecida solução tecnológica especializada de Network Packet Broker (NPB), juntamente com equipamentos de coleta de tráfego, normalmente conhecidos no mercado como “Network TAP’s” e “Bypass Switches”, que terão o objetivo de garantir a visibilidade completa (Leste-Oeste e Norte-Sul) e ininterrupta dos dados trafegados na rede da CMB;

5.2.1.1. Entende-se solução especializada como dispositivos amplamente comercializados e reconhecidos no mercado para tal finalidade, não sendo aceitas soluções similares, tais como: switches comuns, roteadores, balanceadores, servidores genéricos, soluções híbridas, entre outros;

5.2.1.2. Todos os equipamentos (NPB, Networks TAP’s e Bypass Switches) deverão ser **instalados nas premissas da CMB (on-premise)**, em local denominado pela CMB, de acordo com as melhores práticas designadas pelo fabricante;

5.2.1.3. Deverá ser **fornecido Network Packet Broker (NPB) físico (appliance)** acompanhado de kit de montagem compatíveis com rack padrão 19” (dezenove polegadas), contendo as seguintes especificações mínimas:

NETWORK PACKET BROKER (NPB)	
QUANTIDADE: 1 (uma) unidade	
LOCALIDADE: Unidade Santa Cruz	
ATRIBUTO	**ESPECIFICAÇÃO**

Interface de gerenciamento	1x 1 Gbps cobre RJ45 (uma porta de um gigabit por segundo padrão RJ45)
Interfaces destinadas aos Networks TAP's e Bypass Switches físicos	**Quantidade variável**: Deverão ser incluídos/habilitados a quantidade de portas mínimas compatíveis e suficientes para inspecionar/interceptar corretamente o tráfego em consonância com o quantitativo de Networks TAP's e Bypass Switches físicos demandados.
Interfaces destinadas para recebimento do tráfego tunelado dos TAP's Virtuais	2x 10 Gbps fiber singlemode LC (duas portas de dez gigabits por segundo para fibra monomodo padrão LC)
Interfaces destinadas para envio do tráfego ao appliance de NDR (Sensor Físico - TIPO I)	2x 10 Gbps fiber singlemode LC (duas portas de dez gigabits por segundo para fibra monomodo padrão LC)
Interfaces destinadas para uso futuro	1x 10 Gbps fiber singlemode LC (uma porta de dez gigabits por segundo para fibra monomodo padrão LC) 1x 1 Gbps cobre RJ45 (uma porta de um gigabit por segundo padrão RJ45)
Fonte de Energia	2 fontes 100-240V (hot-swap)
Certificação	FIPS 140-2

5.2.1.4. Deverão ser **fornecidos Networks TAP's físicos, que permita conexão de fibra monomodo (singlemode)** através de conectores do tipo LC (Lucent Connector) e suporte velocidade de 10 Gbps (dez gigabits por segundo), em quantidade suficiente para inspecionar/interceptar **até 2 (dois) enlaces de fibra (Tx/Rx) presentes na rede da CMB**;

5.2.1.5. Deverão ser **fornecidos Bypass Switches físicos, que permita conexão de fibra monomodo (singlemode)** através de conectores do tipo LC (Lucent Connector) e suporte velocidade de pelo menos 10 Gbps (dez gigabits por segundo), em quantidade suficiente para inspecionar/interceptar **4 (quatro) enlaces de fibra (Tx/Rx) presentes na rede da CMB**. Alternativamente, os Bypass Switches

poderão ser fornecidos de forma acoplada (módulos) no próprio appliance do Network Packet Broker (NPB) ofertado;

5.2.1.6. Deverão ser **fornecidos TAP's virtuais (vTAP) ou equivalente** (compatíveis com hypervisor VMWare), em quantidade suficiente para inspecionar/interceptar **até 14 (quatorze) servidores físicos (hypervisor) com 450 (quatrocentos e cinquenta) máquinas virtuais** OU suportar **até de 50 TB (cinquenta terabytes) de tráfego por dia**, independentemente da quantidade de vTAP's utilizados no ambiente;

5.2.1.7. Deverão ser **fornecidos chassis, compatíveis com rack padrão 19" (dezenove polegadas), em quantidade suficiente para fixação dos respectivos Networks TAP's e Bypass Switches físicos fornecidos**, devendo ser montados de forma a ocupar o mínimo de espaço (preferencialmente 1U por conjunto de equipamentos);

5.2.1.8. Todos os equipamentos (NPB, Networks TAP's e Bypass Switches), caso necessário, devem vir acompanhados com seus respectivos transceivers em quantidade suficiente para sua plena interconexão e inspeção do tráfego, de acordo com as especificações estabelecidas neste documento;

5.2.1.9. Deverão ser **fornecidos 4 (quatro) cordões de fibra single mode LC**, com tamanho mínimo de 4 (quatro) metros, para cada Network TAP e Switches Bypass de fibra instalado;

5.2.1.10. Deverão ser **fornecidos 4 (quatro) cabos de cobre (padrão CAT 6)** para cada Network TAP de cobre instalado, contendo um tamanho mínimo de 4 (quatro) metros;

5.2.1.11. Os appliances de NPB e Bypass Switches fornecidos deverão possuir homologação vigente junto à Agência Nacional de Telecomunicações (ANATEL);

5.2.1.12. Os appliances de NPB e os TAPs virtuais (vTAPs) fornecidos deverão dispor de console de administração centralizada, composta por interface gráfica (Graphical User Interface – GUI) acessível por meio de navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.).

5.2.2. O Network Packet Broker (NPB) deverá ter a capacidade de agregar o tráfego proveniente dos “Networks TAP’s” (físicos e virtuais) e Switches Bypass, além de eventual “Port Mirroring” (Switch Port Analyzer - SPAN) de switches preexistentes no ambiente da CMB, permitindo que os fluxos de pacotes coexistam simultaneamente;

5.2.2.1. O NPB deverá possuir opção para gerenciamento via linha de comandos (Command Line Interface - CLI);

5.2.2.2. Deve fazer uso de protocolos seguros para comunicação criptografada entre os diferentes componentes da solução, assim como para o acesso à sua console de administração;

5.2.2.3. Deve contar com Application Programming Interface (API) RESTful para permitir a integração eficiente com outras aplicações e serviços;

5.2.2.4. Deve permitir autenticação Single Sign-On (SSO) integrada com os serviços do Active Directory Domain Services (AD DS) ou com o Microsoft Entra ID, o que poderá ocorrer através de um ou mais protocolos padrão de mercado, tais como: RADIUS, LDAP, SAML, OAuth, Kerberos, etc;

5.2.2.5. Permitir que usuários recebam permissões específicas com base em suas funções (Role-Based Access Control - RBAC);

5.2.2.6. Gerar e manter, pelo período mínimo de 30 (trinta) dias, o histórico completo de trilhas de auditoria que permita o rastreamento dos acessos executados por todos os usuários (logs);

5.2.2.7. Deverá permitir que o acesso simultâneo de pelo menos 10 (dez) usuários para administração da solução, desde que devidamente licenciados;

5.2.2.8. Apresentar compatibilidade para atuação em modo de Alta Disponibilidade (High Availability – HA);

5.2.2.9. Permitir monitoramento via Simple Network Management Protocol (SNMP) versão 2 e 3, incluindo a geração de TRAPs para envio de alertas automáticos;

5.2.2.10. Permitir a integração com servidores RADIUS para tarefa de Autorização, autenticação e auditoria (Authentication, Authorization, and Accounting – AAA);

5.2.2.11. Permitir o encaminhamento de logs de auditoria via protocolo SYSLOG para endereço IP de preferência do administrador;

5.2.2.12. Deve contar com uma arquitetura de perda zero de pacotes e capacidade de processamento “Line Rate” (non-blocking/wirespeed) em todas as interfaces para encaminhamento do tráfego;

5.2.2.13. Capacidade de implantar diferentes métodos de encaminhamento de tráfego (1:1, N:N, N:1, 1:N);

5.2.2.14. Capacidade de trabalhar simultaneamente no modo “inline” (inserido no caminho do tráfego) e “out-of-band” (apenas recebendo cópias dos pacotes);

5.2.2.15. Suporte personalizável para configuração de heartbeat (HB) de modo a detectar e se recuperar automaticamente de possíveis falhas nas soluções de segurança inline programadas para receber o tráfego, permitindo a atribuição de heartbeat exclusivos para cada solução (bypass lógico);

5.2.2.16. Permitir a expansão das suas interfaces através da adição de módulos ou licenças, sem impactar o desempenho dos equipamentos ofertados e com todas as portas ofertadas ativadas e licenciadas para todas as funcionalidades solicitadas;

5.2.2.17. Permitir que os pacotes coletados sejam direcionados para ferramentas instaladas em appliances físicos ou máquinas virtuais.

5.2.3. O Network Packet Broker (NPB) deverá capturar e tratar o tráfego antes de encaminhá-los para análise das soluções de segurança e monitoramento de interesse da CMB, devendo vir habilitado com, no mínimo, as seguintes funcionalidades:

I. **Desduplicação (Deduplication):** Descartar pacotes duplicados, de forma a reduzir a quantidade de dados redundantes enviados para as ferramentas de análise e monitoramento;

II. **Rotulagem de Pacotes (Source Port Labeling):** Adicionar rótulos aos pacotes com relação a sua origem (indicação da porta de entrada), de forma a facilitar o rastreamento de onde os dados estão vindo;

III. **Balanceamento de Carga (Load Balancing):** Dividir e distribuir o tráfego de saída entre diversas ferramentas de análise e monitoramento, disponibilizando minimamente as técnicas de balanceamento baseado em peso (weighted) e Round Robin;

IV. **Filtragem de Pacotes (Packet Filtering):** Identificar padrões nos pacotes de rede, permitindo a filtragem do tráfego com base em critérios selecionados, de forma a encaminhar apenas o tráfego de interesse para atender às necessidades das ferramentas de análise e monitoramento;

V. **Fatiamento de Pacotes (Packet Trimmig ou Packet Slicing):** Remover o payload dos pacotes, de forma a preservar apenas seu cabeçalho, permitindo que as ferramentas de análise e monitoramento recebam menos volume de tráfego e que os dados sensíveis fiquem seguros;

VI. **Mascaramento de dados (Data Masking):** Identificar e substituir dinamicamente um conteúdo específico do pacote antes do seu encaminhamento para as ferramentas de análise e monitoramento, mantendo a conformidade regulatória para os dados confidenciais sem remover o payload do pacote, devendo ser compatível minimamente com técnicas de deslocamento relativo (relative offset) e deslocamento estático (static offset) para o início do mascaramento do pacote;

VII. **Tunelamento (Tunneling):** Criar túneis criptografados (L2GRE e/ou VxLAN) para comunicação segurara entre o NPB e os Networks TAP's virtuais;

VIII. **Geração de NetFlow:** Possuir suporte a recursos de geração de NetFlow;

IX. **Identificação de Aplicativos (Application Identification):** Possuir suporte a recursos para identificação de aplicativos na rede;

X. **Descriptografia TLS/SSL (TLS/SSL Decryption):** Realizar a descriptografa do tráfego, permitindo que as ferramentas de análise e monitoramento consigam realizar uma inspeção mais profunda em busca de ameaças.

5.2.4. O Network Packet Broker (NPB) deverá suportar os seguintes throughputs mínimos:

I. **40 Gbps (quarenta gigabits por segundo)** compartilhado entre as funcionalidades de Desduplicação (Deduplication), Fatiamento de Pacotes (Packet Trimmig ou Packet Slicing), Mascaramento de dados (Data Masking) e Tunelamento (Tunneling);

II. **10 Gbps (dez gigabits por segundo)** compartilhado entre as funcionalidades de Identificação de Aplicativos (Application Identification) e Geração de NetFlow;

III. **2 Gbps (dois gigabits por segundo)** para a funcionalidade de Descriptografia TLS/SSL (TLS/SSL Decryption).

5.2.5. O Network Packet Broker (NPB), especificamente com relação a funcionalidade de **Desduplicação (Deduplication),** deverá:

I. Inspecionar o cabeçalho dos pacotes como parâmetros para decisão de similaridade do pacote;

II. Fornecer estatísticas da quantidade de pacotes desduplicados.

5.2.6. O Network Packet Broker (NPB), especificamente com relação a funcionalidade de **Filtragem de Pacotes (Packet Filtering)**, deverá:

I. Identificar padrões em qualquer parte dos pacotes (cabeçalho e payload) das camadas 2 a 4 do modelo OSI;

II. Permitir a criação de filtros personalizáveis e granulares através do uso de operadores lógicos (User Defined Filtering – UDF ou Flow Mapping ou User-defined Attribute - UDA)

III. Permitir definição de filtros utilizando como critérios, no mínimo, os seguintes parâmetros: MAC, VLAN, IPv4, portas TCP/UDP, DSCP, TCP Flags, MPLS, GTP e VxLAN;

IV. Permitir o uso de controle de fluxo simples para direcionar o tráfego por aplicativo ou famílias de aplicativos apenas para ferramentas de monitoramento específicas;

V. Permitir o uso de filtros para indicar que tráfegos específicos não sejam enviados para determinadas ferramentas de análise e monitoramento, incluindo ao menos os seguintes critérios: endereço IP, portas TCP/UDP e VLAN ID;

VI. Permitir a filtragem em campos encapsulados em um túnel, suportando ao menos: GTP, MPLS ou GRE;

VII. Implantar o suporte a overlapping de filtros, ou seja, utilização conjunta de filtros de entrada (ingress) e filtros de saída (egress).

5.2.7. O Network Packet Broker (NPB), especificamente com relação a funcionalidade de **Netflow,** deverá:

I. Suportar ao menos os formatos Netflow v9 e IPFIX;

II. Suportar métodos com amostragem (1:1 ou 1:1000) ou método “sem amostragem” (Unsampled) para análise do tráfego;
III. Dar total visibilidade do tráfego de rede das camadas 2 a 4 do modelo OSI;
IV. Gerar ao menos os seguintes metadados para informações de HTTP: Method, Response Code/Status Code, Version, Host e User Agent;
V. Gerar ao menos os seguintes metadados para informações de DNS: Query Name. Query Type, Response Name, Response IPv6/IPv4;
VI. Gerar ao menos os seguintes metadados para informações de SSL: Certificate Issuer, Certificate CN, Version e Cipher.

5.2.8. O Network Packet Broker (NPB), especificamente com relação a funcionalidade de **Identificação de Aplicativos (Application Identification),** deverá:

I. Identificar e monitorar os aplicativos (camada 7), com base em sua assinatura (ou seja, sem a necessidade de vinculação de porta padrão ou expressões regulares), que passam pela rede, sejam eles comuns ou proprietários;
II. Contar com uma base de dados, atualizada regularmente, com ao menos 1000 (mil) assinaturas de aplicativos conhecidos;
III. Monitorar e relatar o consumo de largura de banda dos principais aplicativos identificados em um período selecionado;
IV. Exibir as estatísticas de tráfego em bytes, pacotes e fluxos dos aplicativos identificados em um período selecionado;
V. Categorizar os aplicativos identificados em grupos (famílias de aplicativos);
VI. Permite a filtragem de tráfego com base no aplicativo (Ex. YouTube, Netflix, Facebook, etc.) ou família de aplicativos (Ex. antivírus, web, ERP, etc.).

5.2.9. O Network Packet Broker (NPB), especificamente com relação a funcionalidade de **Descriptografia TLS/SSL (TLS/SSL Decryption),** deverá:

I. Contar com recurso de descriptografia TLS (Transport Layer Security) e SSL (Secure Sockets Layer) que poderão ser habilitados para qualquer aplicativo;

II. Permitir o monitoramento do tráfego criptografado na rede, onde deverá identificar e descriptografar automaticamente o tráfego antes de entregá-lo às soluções de análise e monitoramento;
III. Permitir o uso de criptografia para o encaminhamento do tráfego, caso seja de interesse do administrador, atuando como um gateway Man-In-The-Middle (MITM);
IV. Permitir descriptografia SSL/TLS do tráfego, alimentando ferramentas que atuam em modo inline (ativa) ou out-of-band (passiva), independentemente da origem do tráfego (interno ou externo);
V. Ter a capacidade de descriptografar cifras Perfect Forward Secrecy (PFS), tais como: ECDHE-RSA-AES256-SHA384 e DHE-RSA-AES128-SHA256;
VI. Permitir configuração de política com base em critérios como endereços IP, domínios, portas TCP/UDP e categorias de URL, podendo os mesmos também serem utilizados para estabelecer regras de exceção da ação da descriptografia;
VII. Permitir que ao menos 1000 (mil) conjuntos certificado/chaves privadas sejam armazenados de forma criptografada na solução;
VIII. Permitir a validação de certificados via Online Certificate Status Protocol (OSCP) ou Certificate Revocation List (CRL);
IX. Possuir suporte aos seguintes protocolos, algoritmos e cifras: SSLv3, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, RSA, ECDSA, ECDH, 3DES, AES, SHA, SHA256 e SHA384;
X. Fornecer estatísticas em tempo real para sessões descriptografadas: conexões SSL/TLS ativas, volume do tráfego SSL/TLS e erros de descriptografia;
XI. Possuir capacidade integração com dispositivos HSM (Hardware Security Module) externos, de forma a verificar as chaves e certificados armazenados de forma centralizada nesses dispositivos;
XII. Processar, no mínimo, 100.000 (cem mil) sessões concorrentes SSL/TLS (inline), considerando toda a orquestração do tráfego (abertura, direcionamento e recriptografia do tráfego). Considera-se 1 (uma) sessão a comunicação bi-direcional fim a fim entre as partes (cliente -> servidor / servidor -> cliente).

5.2.10. Os Networks TAP's (fibra e cobre) e Bypass Switches deverão fornecer acesso não intrusivo aos dados que passam pela rede física da CMB, o que significa que eles não poderão interromper ou altera o tráfego, garantindo que a integridade dos dados não seja comprometida;

5.2.10.1. Os Networks TAP's deverão ter a capacidade de enviar cópias do tráfego (espelhar o tráfego de rede), reproduzindo exatamente os pacotes de dados que passam pela rede em ambas as direções em link full-duplex;

5.2.10.2. Os Bypass Switches deverão atuar de forma "in line" (em linha), onde o tráfego passa pelo dispositivo de forma transparente, permitindo que as soluções de segurança ou monitoramento analisem os dados sem impactar o desempenho da rede. Deve possibilitar que o tráfego de rede continue fluindo mesmo quando as soluções de análise e monitoramento estejam sendo instaladas, desconectadas ou falharem;

5.2.10.3. Os Networks TAP's (cobre apenas) e os Bypass Switches deverão permitir seu monitoramento (via SNMP versão 2 e 3) e gerenciamento remoto (via CLI e GUI), fazendo o uso de interface dedicada (out-of-band) OU por dentro da própria rede monitorada (in-band). No caso dos Bypass Switches, esse requisito **estará dispensado** caso sejam fornecidos de forma acoplada (módulos) no próprio appliance do NPB;

5.2.10.4. Os Networks TAP's (fibra e cobre) e Bypass Switches deverão possuir portas dedicadas para o encaminhamento do tráfego monitorado (monitor/tool ports). No caso dos Bypass Switches, esse requisito **estará dispensado** caso sejam fornecidos de forma acoplada (módulos) no próprio appliance do NPB;

5.2.10.5. Os Networks TAP's (cobre apenas) e os Bypass Switches deverão contar com LEDs para indicar atividade de link das portas e status de energia;

5.2.10.6. Os Networks TAP's (fibra e cobre) e Bypass Switches deverão contar com mecanismo automático para garantir que o tráfego de rede continue fluindo sem interrupções, mesmo no caso da sua falha.

5.2.11. Os **virtual TAP's (vTAP)** deverão fornecer acesso não intrusivo aos dados que passam pela rede virtual da CMB (vSwitch), o que significa que eles não

poderão interromper ou altera o tráfego, garantindo que a integridade dos dados não seja comprometida;

5.2.11.1. Deverão ter a capacidade de interceptar o tráfego lateral gerado entre as Máquinas Virtuais (VM) dentro do ambiente de virtualização (hypervisor), encaminhando uma cópia para o Network Packet Broker (NPB) físico instalado na CMB através de túnel criptografado;

5.2.11.2. Os vTAP's deverão ser compatíveis minimamente com VMware ESXi e VCenter, podendo ser implementados de duas formas distintas:

I. Por meio de Máquina Virtual de Serviço (Service Virtual Machine - SVM), tendo a capacidade de ser comissionada/provisionada e descomissionada/removida automaticamente, de forma a receber apenas o tráfego espelhado dos switches virtuais (vSwitch) no qual possuam Máquinas Virtuais alvo do monitoramento (compatível inclusive com realocação de VM baseada em vMotion);

OU

II. Por meio de "agente" (ou equivalente) instalado diretamente no sistema operacional das Máquinas Virtuais alvo do monitoramento. O agente instalado deve ser único, ou seja, não será permitido a instalação de múltiplos agentes para gerenciar diferentes funcionalidades da solução. Além disso, deve causar o mínimo impacto possível no consumo de recursos de hardware da estação, assegurando que o desempenho geral do sistema não seja comprometido.

5.2.11.3. A CONTRATADA não poderá ter acesso administrativo ao ambiente de virtualização da CMB, cabendo à mesma apenas orientar os profissionais da CMB quanto a correta instalação, configuração e funcionamento dos vTAP's;

5.2.11.4. A solução deverá permitir a definição de quais tipos de protocolos deverão ser interceptados pelos vTAP's para direcionamento ao NPB, proporcionando uma melhor otimização do tráfego a ser copiado;

5.2.11.5. Deverá possibilitar que os vTAP's possam ser utilizados, a critério da CMB, em ambiente de Nuvem Privada (VMWare), Nuvem Pública (mínimo AWS, Azure e GCP) e contêiner baseado em Docker, desde

respeitados os quantitativos de licença solicitados neste Termo de Referência;

5.2.11.6. Os vTAPs deverão ser implementados de forma distribuída, abrangendo todos os nós físicos que compõem os clusters VMware gerenciados, de modo a evitar a concentração da carga de processamento e coleta de tráfego em um único host, assegurando o balanceamento da solução e a adequada visibilidade do ambiente virtual.

5.2.12. Todos os componentes ofertados (NPB, Networks TAP's, Bypass Switches e TAP's virtuais) devem apresentar compatibilidade para trabalhar de forma totalmente integrada.

5.3. CYBER THREAT INTELLIGENCE PLATFORM (CTI)

5.3.1. A solução tecnológica ofertada, ou o conjunto de soluções integradas, deverá ter a capacidade de coletar, analisar e fornecer informações sobre ameaças cibernéticas externas que possam impactar a segurança da CMB, além de realizar o monitoramento para identificar e responder ameaças que possam afetar a reputação e identidade digital da organização. Para tanto, a solução deverá contemplar, no mínimo, as seguintes funcionalidades:

I. Cyber Threat Intelligence;
II. Brand Protection;
III. Supply Chain Risk Management (SCRM);
IV. External Attack Surface Management (EASM).

5.3.2. Deverá ter a capacidade de avaliar ao menos **50 (cinquenta) ativos expostos na internet,** possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais ativos conforme sua preferência, desde que respeitado o limite estabelecido;

5.3.3. Deverá ter a capacidade de realizar o monitoramento de ao menos **4 (quatro) domínios**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais domínios conforme sua preferência, desde que respeitado o limite estabelecido;

5.3.4. Deverá ter a capacidade de realizar o monitoramento de ao menos **5 (cinco) usuários de alto perfil/valor (VIP/executivos)**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais usuários conforme sua preferência, desde que respeitado o limite estabelecido;

5.3.5. Deverá permitir a execução, a critério da CMB, de ao menos **10 (dez) ações de takedown por ano**, compreendendo todas as etapas necessárias para a identificação, solicitação e efetiva remoção de conteúdos que representem riscos à imagem institucional, segurança da informação ou à integridade dos ativos digitais da CMB;

5.3.6. Deverá ter a capacidade de **monitorar a própria CMB** e ao menos **20 (vinte) empresas terceiras** de seu interesse, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais empresas conforme sua preferência, desde que respeitado o limite estabelecido;

5.3.7. Deverá ser dotada de console de administração centralizada, contemplando uma interface gráfica (Graphical User Interface - GUI) acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.);

5.3.8. Deverá fazer uso de protocolos seguros para comunicação criptografada entre os diferentes componentes da solução, assim como para o acesso à sua console de administração;

5.3.9. Deverá contar com Application Programming Interface (API) RESTful para permitir a integração eficiente com outras aplicações e serviços;

5.3.10. Deverá permitir autenticação Single Sign-On (SSO) integrada com os serviços do Active Directory Domain Services (AD DS) ou com o Microsoft Entra ID, o que poderá ocorrer através de um ou mais protocolos padrão de mercado, tais como: RADIUS, LDAP, SAML, OAuth, Kerberos, etc;

5.3.11. Deverá permitir a habilitação de autenticação por multifator (Multi-Factor Authentication - MFA) de terceiros ou do próprio fabricante para gerenciamento da solução;

5.3.12. Deverá permitir que usuários recebam permissões específicas com base em suas funções (Role-Based Access Control - RBAC);

5.3.13. Deverá gerar e manter, pelo período mínimo de 30 (trinta) dias, o histórico completo de trilhas de auditoria que permita o rastreamento dos acessos executados por todos os usuários (logs);

5.3.14. Não poderá apresentar limitação quanto ao número de acessos simultâneas autorizados a administrar a solução, desde que devidamente licenciados;

5.3.15. Deverá contar com suporte de Inteligência Artificial (Artificial Intelligence – IA) para reduzir a ocorrência de falsos positivos;

5.3.16. A funcionalidade de Cyber Threat Intelligence deverá fornecer insights selecionados acerca de ameaças, permitindo um entendimento aprimorado dos vetores de ataque, do comportamento dos agentes maliciosos e dos possíveis alvos, viabilizando, assim, uma avaliação mais acurada dos riscos existentes, a antecipação de potenciais ataques e a tomada de decisões estratégicas das defesas necessárias;

5.3.16.1. Deve fornecer informações detalhadas de inteligência sobre as ameaças cibernéticas globais, ataques, agressores e notícias relativas à segurança cibernética, não apenas da superfície da web, mas também das plataformas ilegais da dark web;

5.3.16.2. Deve identificar a exposição de informações da CMB através do monitorando contínuo da Surface Web e Dark Web. Quanto ao monitoramento da surface Web, para identificação de vazamentos de dados, deve ao menos: Realizar pesquisas em repositório de código (Ex. Github e Bitbucket), realizar buscas em serviço de análise de malware (Ex. AnyRun e Virustotal), pesquisar em armazenamentos públicos (Ex. Amazon Bucket);

5.3.16.3. Deve apresentar pontuação de risco de ameaça, permitindo a avaliação do risco real associado às vulnerabilidades, com base em elementos como mídias sociais, notícias, repositórios de código, Dark/Deep Web e atribuição com atores de ameaças;

5.3.16.4. Deve detectar servidores de Command and Control (C2) utilizados por cibercriminosos, juntamente com o tipo de ataque cibernético, mediante detecção de botnets e malware;

5.3.16.5. Deve relatar botnets detectadas, os endereços IP dos centros de Command and Control (C2) aos quais o malware está conectado e os nomes de domínio falsos, devendo ter a capacidade de compartilhar informações com tecnologias de segurança da CMB para que os IPs de botnet sejam observados nas ferramentas de controle;

5.3.16.6. Deve relatar o resumo digital do arquivo (hash), as informações de reputação da botnet e do malware, como um IoC;

5.3.16.7. Deve apresentar feeds de URL de phishing, APT, botnet, ransomware, malware, sites hackeados e IP em lista negra,

permitindo aplicar filtro nos feeds com o objetivo de utilizá-los nas tecnologias de segurança da CMB;

5.3.16.8. Deve disponibilizar a visualização e pesquisa dos feeds de inteligência sobre ameaças na plataforma;

5.3.16.9. Deve monitorar ameaças relacionadas a setores e regiões geográficas específicas, tendências geográficas na atividade de agentes de ameaças e regiões-alvo;

5.3.16.10. Deve monitorar o comportamento dos atores de ameaças (Threat Actors)/grupos APT (Advanced Persistent Threat) e fornecer como feeds as informações sobre Táticas, Técnicas e Procedimentos (Tactics, Techniques and Procedures - TTP), permitindo sua integração às tecnologias de segurança da CMB;

5.3.16.11. Deve detectar e monitorar nomes de domínio falsificados/phishing que estão preparados para serem usados em ataques de phishing;

5.3.16.12. Deve fornecer o histórico de ataques e dados de hacktivismo do criminoso ou grupo criminoso cibernético;

5.3.16.13. Deve fornecer acesso às informações atualizadas de IoC e TTP sobre os atores de ameaças escolhidos pela CMB;

5.3.16.14. Deve fornecer informações sobre tendências de vulnerabilidades, destacando as mais recentes e críticas, classificadas por produtos e fornecedores;

5.3.16.15. Deve disponibilizar atualizações diárias (redes sociais, Deep web, notícias) sobre os atores de ameaças (grupos APT) escolhidos pela CMB;

5.3.16.16. Deve fornecer relatórios administrativos, resumidos e informativos, bem como relatórios técnicos detalhados;

5.3.16.17. Quanto a caça a ameaças (Threat Hunting), deve fornecer resultados da dark web e da surface web pesquisáveis e fáceis de encontrar.

5.3.17. A funcionalidade de Brand Protection deverá realizar o monitoramento contínuo para identificar proativamente ao uso indevido e falsificação da identidade digital da CMB, visando proteger o valor, confiança, integridade e a reputação da sua marca;

5.3.17.1. Deve conduzir o monitoramento para a proteção do valor da marca da CMB para ao menos as seguintes plataformas: GitHub, GitLab,

Bitbucket, Instagram, Twitter, Telegram, ICQ, IRC, Discord, Pastebin, YouTube, SurfaceWeb, DarkWeb, Rogue Mobile;

5.3.17.2. Deve fornecer rastreamento de notícias ou conteúdo que possam prejudicar o valor da marca da CMB, fornecendo notificações de riscos;

5.3.17.3. Deve fazer buscas no mercado negro com o objetivo de encontrar dados sendo indevidamente comercializado com menção ao domínio da CMB;

5.3.17.4. Deve monitorar continuamente dados, e-mail e credenciais comprometidas relacionadas à CMB expostos em buckets públicos (Ex. Amazon Bucket) e repositório de código (Github);

5.3.17.5. Deve monitorar continuamente domínios falsos que se passam pelo domínio original da CMB (typosquatting e phishing), devendo exibir ao menos as seguintes informações: nome de domínio e tipo de ameaça;

5.3.17.6. Deve permitir adicionar palavras-chave sensíveis para a CMB e pesquisar essas palavras-chave nos canais: GitHub, GitLab, Bitbucket, Instagram, Twitter, Telegram, ICQ, IRC, Discord, Pastebin, YouTube, SurfaceWeb e DarkWeb;

5.3.17.7. Deve monitorar continuamente perfis que se passam pelos perfis de mídia social da CMB, como plataformas de mídia social X (antigo Twitter), Facebook e Instagram. Deverão ser exibidas ao menos as seguintes informações sobre os perfis identificados: Nome do perfil, identificador (Handle name) e contagem de amigos/seguidores;

5.3.17.8. Deve monitorar continuamente as principais lojas de aplicativos para identificar aplicativos falsos semelhantes aos oficiais da CMB, devendo minimamente disponibilizar a URL para download do aplicativo falso;

5.3.17.9. Deve monitorar continuamente o vazamento ou exposição de dados pessoais e profissionais de indivíduos de alto perfil/valor (VIP/executivos) em busca de atividade maliciosa;

5.3.17.10. Deve ter a capacidade de gerar alarmes para indicar quando violações forem detectadas;

5.3.17.11. Deve possuir recurso integrado para realização de remoção/derrubada (takedown) de domínios fraudulentos, tomando

as medidas cabíveis mediante a aprovação da CMB, além de possibilitar o rastreamento do processo de takedown e o monitoramento da reabertura dos domínios removidos.

5.3.18. A funcionalidade de Supply Chain Risk Management (SCRM) deverá monitorar proativamente postura de segurança de empresas terceiras relevantes para a CMB (fornecedores, fabricantes, parceiros e prestadores de serviços), com o objetivo de identificar potenciais riscos cibernéticos que possam comprometer a organização;

5.3.18.1. Deve fornecer informações sobre os perfis de cada uma das empresas monitoradas, incluindo o cálculo do seu score de popularidade e níveis de exposição cibernética, o que deverá ocorrer de forma dinâmica de acordo com os dados coletados;

5.3.18.2. Deve calcular o nível de exposição das empresas monitoradas com base na combinação de informações coletadas na superfície da web e dark web;

5.3.18.3. Deve possuir sistema de alarmes sobre eventos críticos, garantindo que riscos potenciais ou desenvolvimentos notáveis na cadeia de suprimentos sejam notificadas;

5.3.18.4. Deve permitir a atribuição de tags às empresas monitoradas e personalizar alarmes para facilitar o gerenciamento;

5.3.18.5. Deve monitorar vulnerabilidades que afetam fornecedores específicos indicados pela CMB, possibilitando inclusive o recebimento de alertas;

5.3.18.6. Deve permitir buscas de empresas com base nos seguintes critérios mínimos: nome, domínio, setor de negócio e país. Adicionalmente, deverá incluir obrigatoriamente filtros específicos para o setor "Administração Pública" (ou similar) e para o país "Brasil";

5.3.18.7. Deve detectar automaticamente e recomendar potenciais empresas terceiras que tenham relação com o negócio da CMB, classificando-as em categorias com base em sua localização geográfica e alcance;

5.3.18.8. Deve possuir relatórios de segurança dinâmicos relacionados às empresas monitoradas, possibilitando inclusive gerar relatórios específico para cada uma delas. Este relatório deverá conter ao menos as seguintes informações: domínio principal, endereços IP relacionados e descrição da companhia;

5.3.18.9. Deve permitir explorar e analisar dados das empresas monitoradas, viabilizando o acesso rápido a páginas relevantes, informações gerais e insights abrangentes de notícias;

5.3.18.10. Deve permitir revisar as informações gerais das empresas monitoradas, incluindo o histórico de relatórios gerados anteriormente e as últimas notícias relacionadas;

5.3.18.11. Deve fornecer atualizações instantâneas sobre ao menos três tipos distintos de notícias de segurança cibernética: ransomware, ataques cibernéticos e defacement;

5.3.18.12. Deve fornecer ao menos as seguintes informações de segurança relacionadas às empresas monitoradas: vulnerabilidades, nível de risco, recomendações para correção, data da detecção, credenciais comprometidas, fraudes com a marca, usuários infectados por artefatos maliciosos;

5.3.18.13. Deve apresentar informações encontradas na Deep e Dark Web relativas às empresas monitoradas, devendo conter minimamente as informações da data e origem das menções;

5.3.18.14. Deve permitir classificar as empresas monitoradas em categorias, possibilitando concentrar os esforços de segurança nas empresas de maior relevância para os objetivos estratégicos da CMB;

5.3.18.15. Deve possuir uma linha do tempo que possibilidade visualizar o histórico de ataques voltados às empresas monitoradas, possibilitando inclusive filtrar por com base no país ou tipo de ataque para uma análise mais granular;

5.3.18.16. Deve analisar constantemente o cenário de ameaças em busca de atividades suspeitas e potenciais vulnerabilidades relativas às empresas monitoradas, incluindo o monitoramento de feeds de notícias, alertas de segurança e tendências do setor.

5.3.19. A funcionalidade de External Attack Surface Management (EASM) deverá realizar a descoberta automática de ativos da CMB expostos na internet (sites, servidores de e-mail, serviços em nuvem, aplicativos WEB, entre outros), sejam eles conhecidos ou desconhecidos, proporcionando uma visibilidade completa quanto as vulnerabilidades associadas a cada ativo descoberto

5.3.19.1. Deve identificar, no mínimo, softwares vulneráveis, software de terceiros, certificados SSL expirados e registros DNS;

5.3.19.2. Deve automaticamente classificar os ativos expostos em diferentes tipos ou grupos;

5.3.19.3. Deve permitir a exclusão manual de determinados ativos expostos do monitoramento;

5.3.19.4. Deve gerar uma pontuação de risco para os ativos expostos, devendo ser calculado de forma dinâmica com base nas informações coletadas, a fim de priorizar a sua remediação;

5.3.19.5. Deve permitir a atribuição de TAGs customizadas aos ativos expostos para facilitar a sua identificação e controle;

5.3.19.6. Deve permitir buscas pelos ativos expostos, possibilitando minimamente o uso dos seguintes filtros: tipos/grupos de ativos, nome do ativo, data da descoberta e TAGs associadas;

5.3.19.7. Deve realizar varreduras ativas (com ataques conhecidos) para encontrar potenciais vulnerabilidades nos ativos expostos, além da capacidade de utilizar técnicas de varreduras ativa e passiva para identificar portas de comunicação abertas;

5.3.19.8. Deve automaticamente gerar alertas referentes às vulnerabilidades identificadas, devendo minimamente listar as seguintes informações: Identificador CVE, descrição, severidade, data da descoberta e ativos afetados;

5.3.19.9. Deve permitir o envio dos alertas para caixas de e-mails específicas, a critério do administrador;

5.3.19.10. Deve permitir associar alarmes para operadores específicos cadastrados na solução, além de possibilitar a mudança do status dos alertas conforme o andamento do seu tratamento;

5.3.19.11. Deve demonstrar a lista dos ativos mais vulneráveis, além da quantidade total de vulnerabilidades identificadas no ambiente separados por severidade.

5.3.20. Todo o conjunto de funcionalidades exigidas para a solução tecnológica ofertada deverá operar de forma integrada e interoperável, sem prejuízo da flexibilidade prevista nos itens 1.34, 1.35 e 1.36.

5.4. VULNERABILITY MANAGEMENT PLATFORM

5.4.1. A solução tecnológica ofertada, ou o conjunto de soluções integradas, deverá realizar a avaliação de vulnerabilidades do ambiente tecnológico da CMB. Para tanto, a solução deverá contemplar, no mínimo, as seguintes funcionalidades:

I. Vulnerability Scanning;
II. Web App end API Scanning;
III. Policy Compliance;
IV. Patch Management.

5.4.2. Deverá inventariar e realizar varreduras de vulnerabilidades em múltiplos tipos de ativos, incluindo ao menos:

I. Servidores Windows e Linux (físicos e virtuais);
II. Contêineres Docker;
III. Desktops Windows, Linux e MAC (físicos e virtuais);
IV. Softwares instalados nas estações;
V. Plataforma Hypervisor (mínimo VMware);
VI. Switches, Roteadores e Access Points;
VII. Aplicações Web e APIs;
VIII. Impressoras, câmeras IP e telefones VoIP;
IX. Celulares/tablets (Android, iOS/iPad OS);
X. Certificados TLS/SSL (internos e externos);
XI. Dispositivos OT (Operational Technology) e IoT (Internet of Things).

5.4.3. Deverá ter a capacidade de avaliar ao menos **3.000 (três mil) ativos**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais ativos conforme sua preferência, desde que respeitado o limite estabelecido;

5.4.4. Deverá ter a capacidade de avaliar ao menos **50 (cinquenta) FQDN's**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais FQDN's conforme sua preferência, desde que respeitado o limite estabelecido;

5.4.5. Deverá ter a capacidade de avaliar ao menos **150 (cento o cinquenta) contêineres** e **40 (quarenta) worker nodes**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais contêineres e worker nodes conforme sua preferência, desde que respeitado o limite estabelecido;

5.4.6. Deverá ser dotada de console de administração centralizada, contemplando uma interface gráfica (Graphical User Interface - GUI) acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.);

5.4.7. Deverá fazer uso de protocolos seguros para comunicação criptografada entre os diferentes componentes da solução, assim como para o acesso à sua console de administração;

5.4.8. Deverá contar com Application Programming Interface (API) RESTful para permitir a integração eficiente com outras aplicações e serviços;

5.4.9. Deverá permitir autenticação Single Sign-On (SSO) integrada com os serviços do Active Directory Domain Services (AD DS) ou com o Microsoft Entra ID, o que poderá ocorrer através de um ou mais protocolos padrão de mercado, tais como: RADIUS, LDAP, SAML, OAuth, Kerberos, etc;

5.4.10. Deverá permitir a habilitação de autenticação por multifator (Multi-Factor Authentication - MFA) de terceiros ou do próprio fabricante para gerenciamento da solução;

5.4.11. Deverá permitir que usuários recebam permissões específicas com base em suas funções (Role-Based Access Control - RBAC);

5.4.12. Deverá gerar e manter, pelo período mínimo de 30 (trinta) dias, o histórico completo de trilhas de auditoria que permita o rastreamento dos acessos executados por todos os usuários (logs);

5.4.13. Não poderá apresentar limitação quanto ao número de acessos simultâneas autorizados a administrar a solução, desde que devidamente licenciados;

5.4.14. Deverá realizar varreduras (scanning) de vulnerabilidades com uma taxa de precisão de detecção mínima de 99,99966% (Six Sigma), visando minimizar a ocorrência de falsos positivos. Ao menos as seguintes alternativas de varreduras devem estar presentes na solução:

I. Varredura ativa não autenticada;
II. Varredura ativa autenticada;
III. Varredura com e sem “agente” instalado.

5.4.15. O agente disponibilizado pela solução deverá apresentar compatibilidade para instalação, no mínimo, nas versões dos Sistemas Operacionais (SO) listados abaixo. Mesmo que não seja possível habilitar todas as funcionalidades exigidas, em decorrência de tratar-se de versão

legada/descontinuada, ao menos a função de inventário da solução deve ser compatível com todas as versões apresentadas:

I. Windows 10 e 11;
II. Windows Server 2012, 2012 R2, 2016, 2019, 2022 e 2025;
III. Redhat Enterprise Linux 7 ao 9;
IV. CentOS Linux 9;
V. Ubuntu Linux 16 LTS ao 24 LTS;
VI. Apple MacOS 13 ao 15.

5.4.16. A solução deverá permitir a descoberta e categorização automática de ativos conhecidos e desconhecidos, usando métodos com e sem agente, para a construção de um inventário unificado do ambiente, possibilitando o registro mínimo das seguintes informações:

I. Hostname, localização geográfica, status (online ou offline), tipo (desktop, servidor, etc.), fabricante e modelo;
II. Fully Qualified Domain Name (FQDN);
III. Endereçamento IP e MAC;
IV. Domínio ingressado (Active Directory - AD);
V. Nome, versão, arquitetura (64 ou 32 bits), service pack, kernel do Sistema Operacional Instalado;
VI. Nome, versão e categoria dos serviços internos em execução e dos softwares instalados;
VII. Portas TCP/UDP abertas;
VIII. Vulnerabilidades (CVSS/CVE) e nota de risco;
IX. Memória RAM, processador e volume de disco;
X. Informações sobre os ambientes de contêineres: imagens, registros, contêineres associados (ativos e inativos) e hosts;
XI. Metadados das imagens de contêineres: rótulos, tags e software instalado.

5.4.17. Deverá permitir a criação e atribuição de “TAGs” (etiquetas) nos ativos para facilitar a sua identificação, permitindo a geração de “TAGs”, pelo menos, usando os seguintes parâmetros:

I. Palavras-chave;
II. Endereço IP e intervalos de IP;
III. Portas TCP/UDP abertas;
IV. Sistema operacional;

V. Presença ou ausência de determinado software instalado ou serviço em execução;

VI. Regular Expressions (Regex).

5.4.18. Deverá agrupar automaticamente os ativos por categoria funcional e famílias de produtos, tipo de dispositivo, tipo de plataforma e fabricante, além de permitir o agrupamento manual a critério do administrador;

5.4.19. Deverá normalizar automaticamente os nomes dos fabricantes de hardware e software com seus dados relevantes para facilitar sua posterior busca, por exemplo: a visualização de quantidade de estações com um determinado hardware ou software instalado;

5.4.20. Deverá permitir, a critério do administrador, o agendamento de uma periodicidade para execução contínua das varreduras, além da sua execução manual (On Demand), possibilitando ao menos as seguintes configurações:

I. Inclusão e exclusão de range IP a ser verificado;

II. Inclusão e exclusão de portas TCP/UDP a serem verificadas;

III. Permitir a varredura de ativos que não respondam ping;

IV. Remoção automática de ativos inativos das varreduras;

V. Definição de níveis de desempenho das varreduras, tais como: Alto ou similar (otimizado para velocidade e tempos de varredura mais curtos), normal ou similar (equilibrado entre intensidade e velocidade) e baixo ou similar (otimizado para conexões de rede de baixa largura de banda);

VI. Definição da duração máxima das varreduras por ativo verificado, devendo a verificação no ativo ser abortada automaticamente caso a duração máxima definida seja excedida

VII. Definição de teste de força fruta de senha, possibilitando utilizar uma lista de senhas;

VIII. Definição do tipo de verificação de vulnerabilidade que deve ser executada, tais como: completa (escaneia todas as vulnerabilidades aplicáveis ao ativo) e personalizada (permitir que o administrador selecione uma lista vulnerabilidades específicas);

IX. Permitir a habilitação de verificações intrusivas, ou seja, a solução deverá tentar comprometer a vulnerabilidade;

X. Permitir o fornecimento de credenciais para varreduras autenticadas, possibilitando verificações mais completas;

XI. Permitir o uso de um cabeçalho HTTP personalizado.

5.4.21. Deverá realizar a detecção balanceadores de carga ao executar as varreduras de vulnerabilidades;

5.4.22. Deverá atualizar periodicamente a base de conhecimento de vulnerabilidades, garantindo a incorporação de ao menos 20 (vinte) CVEs, e possuir uma base de conhecimento com, no mínimo, 35.000 (trinta e cinco mil) CVEs relacionados, incluindo tecnologias legadas;

5.4.23. Deverá permitir a realização de varreduras paralelas em diferentes ativos para acelerar o processo e obter resultados mais rapidamente;

5.4.24. Deverá oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL);

5.4.25. Deverá mapear os riscos identificados nas diferentes táticas, técnicas e procedimentos (TTP) do MITRE ATT&CK;

5.4.26. Deverá possuir a capacidade de determinar se o host está ativo e fazer fingerprinting para a descoberta de serviços, devendo inclusive identificar o sistema operacional instalado e executar verificações de vulnerabilidade específicas referentes ao sistema descoberto;

5.4.27. Deverá permitir vincular as vulnerabilidades detectadas e indicar sua relação com ameaças de Malware;

5.4.28. Deverá indicar explorações disponíveis e códigos disponíveis para uma vulnerabilidade, quando aplicável;

5.4.29. Deverá possuir banco de dados capaz de relacionar a maioria das vulnerabilidades ao CVE e Bugtraq;

5.4.30. Deverá utilizar Inteligência Artificial (IA) para realizar análise preditiva das vulnerabilidades, fazendo uso de dados provenientes de bases de Threat Intelligence e feeds de ameaças para auxiliar na priorização da sua correção;

5.4.31. Deverá permitir a correlação em tempo real das ameaças ativas contra as vulnerabilidades detectadas nos ativos corporativos;

5.4.32. Deverá atribuir uma nota de risco aos ativos, de forma a identificar ativos que apresentam maior perigo;

5.4.32.1. As notas de risco deverão sofrer atualizações periódicas para refletir o cenário de ameaças em transformação;

5.4.32.2. A nota de risco Deve ser formada pela pontuação CVSS (Common Vulnerability Scoring System), informações de inteligência de ameaças (Exploit Code Maturity (ECM), agentes de ameaças ativos, malwares associados, possibilidade de remediação e criticidade do ativo (atribuído pela própria CMB);

5.4.32.3. Deve atribuir uma pontuação para cada vulnerabilidade identificada, de forma a quantificar o risco associado a mesma.

5.4.33. Deverá Incluir indicadores de ameaças em tempo real que ajudam a avaliar e priorizar as vulnerabilidades detectadas, categorizados da seguinte forma:

I. Dia Zero;
II. Exploração pública;
III. Ataques ativos;
IV. Movimento lateral;
V. Fácil exploração;
VI. Perda de dados;
VII. Negação de serviço;
VIII. Vulnerabilidade sem patch disponível;
IX. Malware;
X. Kit de exploração.

5.4.34. Deverá realizar verificação de conformidade para analisar se os ativos estão configurados de acordo com as políticas de segurança esperadas;

5.4.34.1. Deve identificar lacunas de segurança baseada, no mínimo, nos seguintes frameworks: ISO 27001 ISMS, Center for Internet Security Benchmarks (CIS), National Institute of Standards (NIST) e Payment Card Industry Data Security Standards (PCI DSS);

5.4.34.2. Deve fisponibilizar ao menos 800 (oitocentos) controles de segurança prontos para uso para identificar configurações incorretas;

5.4.34.3. Deve apresentar capacidade de analisar a conformidade de ambientes de SaaS (Mínimo Microsoft 365).

5.4.34.4. Deve permitir a detecção de falhas de conformidades através de varreduras autenticadas ou através de agente instalado diretamente no ativo monitorado;

5.4.34.5. Deve permitir que o mesmo scanner varra por falhas de conformidade e também por vulnerabilidades.

5.4.35. Deverá descobrir, catalogar e avaliar vulnerabilidades dos aplicativos Web e APIs presentes na rede externa, internas e instâncias de nuvem;

5.4.35.1. Deve detectar e avalia os 10 principais riscos do Open Web Application Security Project (OWASP), ameaças do WASC (Web Application Security Consortium) e fraquezas do CWE (Common Weakness Enumeration);

5.4.35.2. Deve permitir avaliações de segurança por meio de varredura autenticada, simulando interações reais do usuário e utilizando varreduras avançadas fornecer insights profundos;

5.4.35.3. Deve identificar aplicações Web e APIs aprovadas e não aprovadas, gerando um processo contínuo de catalogação e descoberta;

5.4.35.4. Deve permitir a criação de exceções para definir quais partes da aplicação não devem ser varridas pela solução;

5.4.35.5. Deve varrer tanto em aplicações Web que utilizam HTML tradicionais, como em aplicações Web dinâmicas (HTML5, JavaScript e AJAX), incluindo aplicativos de página única (Single Page Applications - SPA);

5.4.35.6. Deve realizar verificação SSL/TLS para analisar se há certificados inválidos, prestes a expirar ou emitidos incorretamente;

5.4.35.7. Deve realizar a verificação das respostas emitidas pelo HTTP para identificar se estão sendo retornadas informações que possam ser utilizadas por agentes maliciosos para explorar vulnerabilidades;

5.4.35.8. Deve permitir varreduras progressivas, permitindo uma varredura em estágios incrementais, de forma a evitar impacto no seu funcionamento.

5.4.36. Além da detecção e priorização das vulnerabilidades, deverá também permitir a aplicação remota de patches, tanto voltados para correção de sistemas operacionais (Windows, Linux e MAC), como para correção de softwares instalados nesses sistemas;

5.4.36.1. Deve permitir o planejamento, execução e acompanhamento de ações de mitigação para as vulnerabilidades encontradas e executadas pela plataforma;

5.4.36.2. Deve possuir fluxos de trabalho automatizados e agendáveis desde a detecção da vulnerabilidade até a execução das ações de remediação e mitigação para os ativos;

5.4.36.3. Deve permitir que a correção ocorra, a critério do administrador, de forma automatizada ou manual (On Demand), possibilitando inclusive o agendamento da correção para execução imediata após a sua identificação, execução única (não recorrente) e de forma recorrente (em data e horário específico). Serão admitidas, em decorrência de limitações técnicas específicas, que excepcionalmente alguns patchs não possam ser aplicados de forma remota, cabendo à solução disponibilizar apenas o link para download do patch (quando disponível);

5.4.36.4. Deve fornecer sugestões de mitigação, vinculando-as com informações de CVEs;

5.4.36.5. Deve permitir a visualização dos detalhes de um patch específico, contendo ao menos as seguintes informações: nome e descrição, nome do fabricante, severidade, tamanho, data da publicação, número do KB/boletim, CVEs associados, lista de ativos nos quais o patch está ausente;

5.4.36.6. Especificamente para os dispositivos Windows, além da instalação dos patches, a solução deverá permitir também a sua reversão (Rolling Back), o que também poderá ocorrer de forma manual (On Demand) ou agendada (em dia e horário definido pelo administrador);

5.4.36.7. Para cada patch disponível, deve ser indicado a necessidade de reinicialização do sistema após a sua aplicação ou reversão, possibilitando ao administrador habilitar o envio de uma mensagem customizáveis aos usuários indicando que uma reinicialização é necessária, dando ao mesmo a opção de adiar ou reiniciar imediatamente a estação. Deverá possibilitar a definição do número máximos de vezes que o adiamento da reinicialização será permitido;

5.4.36.8. Deve permitir selecionar manualmente os patches a serem aplicados através de um filtro de seleção que considere ao menos: severidade do patch, fabricante, associação a uma vulnerabilidade e pontuação de risco de segurança;

5.4.36.9. As ações de mitigação das vulnerabilidades devem refletir nas métricas de risco associadas a uma determinada vulnerabilidade para um determinado ativo;

5.4.36.10. Deve permitir restringir a instalação ou remoção dos patches a um grupo de máquinas baseados em range IP, software instalado e serviços internos em execução;

5.4.36.11. Deve permitir o download de patches antes do início da sua aplicação, de forma a otimizar o processo de instalação;

5.4.36.12. As vulnerabilidades encontradas para cada ativo devem refletir o status de implementação das mitigações propostas, indicando se as mitigações foram implementadas de forma parcial ou total;

5.4.36.13. Deve exibir o status de instalação dos patchs, sinalizando quais foram instalados com sucesso e quais falharam, além do motivo da falha;

5.4.36.14. Deve exibir a quantidade de ativos que possuem um determinado software instalado e quantidade de patches relevantes a esse mesmo software;

5.4.36.15. Especificamente para os dispositivos Windows, deverá permitir a execuções de ações antes e após a aplicação dos patchs, tais como: execução de scripts, instalar/desinstalar software e alterar chave do registro;

5.4.36.16. Deve permitir agendar a execução de tarefas de patch com agendamento a partir do Patch Tuesday, da Microsoft, de forma automática;

5.4.36.17. Deve conter a inteligência de filtrar automaticamente, sem intervenção, quais ativos receberão os patches selecionados na tarefa de patch considerando a arquitetura do sistema operacional e a pré-existência de determinada aplicação, evitando assim instalações indesejadas.

5.4.37. A solução deverá possuir um catálogo com ao menos 35.000 patches, permitir aplicação de patches para, no mínimo, os seguintes produtos/softwares:

7-Zip; Adobe Acrobat; Adobe Flash; Adobe Reader; Adobe Shockwave;	Microsoft Windows XP, 7, 8, 8.1, vista e 10; Microsoft SQL Server 2000 ao 2019; Microsoft Management Studio Express; Microsoft Management Studio 17 e

Apache Tomcat; Apple iCloud; Apple iTunes; Apple Mobile Device Support; Apple Software Update; Box Drive; Box Edit; Box Sync; Cisco Jabber; Cisco WebEx Teams; Citrix GoToMeeting; Citrix Receiver; Citrix Workspace App; Dropbox; FileZilla; GIT GlavSoft TightVNC Google Chrome; Google Drive; Google Desktop; Google Drive File Stream; Google Earth Pro; KeePass; LibreOffice; LogMeIn; Microsoft .Net; Microsoft .Net Core; Microsoft AntiXSS Microsoft Azure Site Recovery Provider; Microsoft Azure Information Protection Client; Microsoft Windows Defender; Microsoft DirectX; Microsoft Dynamics; Microsoft Edge; Microsoft Exchange Server; Microsoft Exchange System Manager;	18; Microsoft System Center Operations Manager; Microsoft Agent System Center Operations Manager; Microsoft Audit Collection Server; Microsoft System Center Operations Manager; Microsoft Console System Center Operations Manager; Microsoft Gateway System Center Operations Manager; Microsoft Reporting System Center Operations Manager Server; Microsoft System Center Operations Manager Web Console; Microsoft System Center Virtual Machine Manager; Microsoft Systems Management Server; Microsoft Visual Studio Code; Microsoft Visual Studio Tools for Applications 2.0; Microsoft Visual Studio .NET; Microsoft Visual Studio .NET 2003; Microsoft Visual Studio 2005 ao 2017; Microsoft Visual Studio Team; Foundation Server 2010 ao 2018; Microsoft WSUS; Mozilla Firefox; Mozilla Thunderbird; Nmap; Notepad++; Opera Browser; VM VirtualBox; Rarlab WinRAR; RealPlayer; RealVNC Free Edition; RealVNC Connect; RealVNC Viewer; PuTTY; Sun Microsystems Java 6 ao 11;

Microsoft Identity Manager; Microsoft Internet Explorer; Microsoft Access 2000 ao 2016; Microsoft Excel 2000 ao 2016; Microsoft Outlook 2000 ao 2016; Microsoft PowerPoint 2000 ao 2016; Microsoft Project 2000 ao 2016; Microsoft Word 2000 ao 2016; Microsoft Excel 2000 ao 2016; Microsoft Visio 2002 ao 2016; Microsoft Visio Viewer 2003 ao 2013; Microsoft OneNote 2010 ao 2019; Microsoft Power BI Desktop; Microsoft PowerShell; Microsoft Server 2000, 2008, 2008 R1, 2012, 2012 R2, 2016 e 2019;	TeamViewer; UltraVNC; VMware Horizon Client; VMware Horizon View Client; VMware Player; VMware Tools; VMware Workstation; WinSCP; WinZip; Wireshark; Zoom Client; Zoom Outlook Plugin;

5.4.38. Deverá possuir "alertas" pré-definidos nativamente na solução, além de permitir a customização de novos, possibilitando inclusive o seu envio automático por email para, no mínimo, os seguintes casos:

I. Quando um escaneamento é concluído, colocado em pausada ou cancelado;

II. Mudanças e vulnerabilidades encontradas no certificado SSL, além de certificados expirados e/ou próximos de expirar;

III. Identificação de vulnerabilidades graves;

IV. Vulnerabilidades que ainda não foram corrigidas após um período específico;

V. Identificação de alteração nas portas TCP/UDP abertas e alteração de serviço rodando na porta;

VI. Identificação de software não aprovado.

5.4.39. Deverá permitir a criação e customização de dashboards e relatórios, além de viabilizar buscas interativas de informações pelo sistema, devendo ter a capacidade de apresentar ao menos:

I. Informações de tendência de vulnerabilidade, incluindo o número total de vulnerabilidades novas, reabertas, ativas e fechadas;

II. Informações de varreduras de vulnerabilidades, incluindo: data e hora de início, duração da verificação, o número total de hosts verificados e o número de hosts ativos (hosts em execução no momento da verificação);
III. Vulnerabilidade identificas por ativo, severidade, categoria, sistema operacional, produto/software. status, CVSS ou CVE;
IV. Quantidade de ocorrências de uma mesma vulnerabilidade;
V. Vulnerabilidades detectadas em um segmento de rede, em serviços específicos e usuário específico;
VI. Vulnerabilidades associadas a ransomware e que possuem patches disponíveis, exploits públicos e que permitem exploração sem autenticação;
VII. Variação histórica de vulnerabilidades novas, corrigidas e reabertas;
VIII. Conformidade dos ativos com os frameworks suportados;
IX. Pontuação de risco e sua variação ao longo do tempo;
X. Patches disponíveis para os ativos, mostramos a data e a hora em que o ativo foi escaneado, o nome do ativo, seu sistema operacional e o número total de patches ausentes;
XI. Ativos que não possuem patches instalados, pendente de boot para aplicação, patches faltantes por fabricante, status da aplicação e patches faltantes por severidade;
XII. Ativos que possuem um software instalado e quantidade de patches relevantes a esse mesmo software;
XIII. No status individual de cada tarefa de patch, mostrar quais patches foram instalados com sucesso, quais não foram instalados por não serem necessários e quais falharam (devendo apontar o motivo do erro);
XIV. Ativos que executam containers e quantidade de containers em execução.

5.4.40. Todo o conjunto de funcionalidades exigidas para a solução tecnológica ofertada deverá operar de forma integrada e interoperável, sem prejuízo da flexibilidade prevista nos itens 1.34, 1.35 e 1.36.

5.5. BREACH AND ATTACK SIMULATION (BAS)

5.5.1. A solução tecnológica ofertada deverá oferecer uma abordagem proativa de análise do ambiente tecnológico da CMB, permitindo avaliar sua postura de segurança através de uma ampla gama de cenários simulados de ataques cibernéticos, não podendo trazer qualquer risco real de infectar a rede da CMB ou impactar suas atividades;

5.5.1.1. As simulações de vetores de ataques deverão auxiliar na identificação de vulnerabilidades e potenciais fraquezas (lacunas de segurança) presentes no ambiente, antes que invasores sofisticados possam explorá-las, permitindo a priorização dos esforços de correção com base no nível de risco;

5.5.1.2. A solução deve funcionar imitando as táticas, técnicas e procedimentos (TTPs) usados por criminosos cibernéticos reais para identificar vulnerabilidades e avaliar a eficácia dos controles de segurança da CMB;

5.5.1.3. Deve apresentar resultados ou informações que possam ser usados diretamente para tomar ações ou medidas práticas, ou seja, que não apenas descreva uma situação, mas que forneçam sugestões práticas sobre como corrigir as vulnerabilidades e lacunas de segurança identificadas.

5.5.2. Deverá ter a capacidade de executar simulações de ataque em todo o parque tecnológico da CMB, permitindo executar ao menos **20 (vinte) simulações por mês**, tendo como alvo qualquer ativo no ambiente, ou seja, a solução não poderá estar vinculada a ativos específicos, podendo ser executada em qualquer conjunto de ativo de interesse da CMB, desde que despeitado o quantitativo máximo mensal estipulado;

5.5.2.1. Deve permitir a execução ilimitada de todos os vetores de simulação disponíveis na plataforma.

5.5.3. Deverá ser dotada de console de administração centralizada, contemplando uma interface gráfica (Graphical User Interface - GUI) acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.);

5.5.4. Deverá fazer uso de protocolos seguros para comunicação criptografada entre os diferentes componentes da solução, assim como para o acesso à sua console de administração;

5.5.5. Deverá contar com Application Programming Interface (API) RESTful para permitir a integração eficiente com outras aplicações e serviços;

5.5.6. Deverá permitir que usuários recebam permissões específicas com base em suas funções (Role-Based Access Control - RBAC);

5.5.7. Deverá gerar e manter, pelo período mínimo de 30 (trinta) dias, o histórico completo de trilhas de auditoria que permita o rastreamento dos acessos executados por todos os usuários (logs);

5.5.8. Não poderá apresentar limitação quanto ao número de acessos simultâneas autorizados a administrar a solução, desde que devidamente licenciados;

5.5.9. A solução, para execução das simulações de vetores de ataques, poderá fazer uso de “agente” instalado nas estações da CMB OU “appliance virtual” OU ambos;

5.5.9.1. O agente deve ser compatível, no mínimo, com sistemas operacionais Windows Desktop (10 e 11), Windows Server (2012 ao 2022) e Linux (Ubuntu 22.04);

5.5.9.2. Deve permitir a execução de simulações a partir de qualquer estação que tenha o agente instalado, com capacidade de fornecer resultados em poucas horas;

5.5.9.3. No caso de utilização de “appliance virtual”, este deverá ser instalado dentro do ambiente de virtualização da CMB (compatível obrigatoriamente com Hypervisor VMWare), atendendo as seguintes condições:

I. O serviço necessário ao seu funcionamento deverá ser compatível para instalação em servidor com sistema operacional Linux ou Windows, a ser fornecido e instalado pela própria CMB, cabendo à CONTRATADA prestar as devidas orientações para a sua correta configuração e funcionamento;

II. No caso do sistema operacional Windows, o servidor fornecido pela CMB será disponibilizado apenas com as licenças Windows Server Datacenter e CAL (Client Access License), cabendo à CONTRATADA o fornecimento de todas as demais licenças necessárias para o correto funcionamento do serviço;

III. Deverá ser instalado atrás do firewall da CMB, em rede de sua conveniência, de acordo com as recomendações do fabricante;

IV. A CMB ficará responsável pelo seu backup e recuperação em caso de eventual incidente que leve a sua indisponibilidade, cabendo ainda à CONTRATADA prestar todo o apoio necessário para viabilizar esse processo.

5.5.10. Deverá possuir biblioteca de simulações de ameaças constantemente atualizada, composta por ao menos 6.000 (seis mil) simulações;

5.5.10.1. Deve disponibilizar base de simulações de malwares mais recentes em até 48 (quarenta e oito) horas após a sua divulgação;

5.5.10.2. As simulações disponibilizadas devem ser primeiramente testadas e validadas em ambiente interno de laboratório do próprio Fabricante da solução, antes da sua disponibilização na plataforma para uso da CMB.

5.5.11. Deverá identificar caminhos genuínos que invasores poderiam utilizar para obter privilégios administrativos ou comprometer o ambiente;

5.5.11.1. Deve identificar e priorizar pontos críticos obtidos através das simulações;

5.5.11.2. Deve apresentar compatibilidade com Microsoft Active Directory para apontar caminhos de ataque que poderiam permitir o seu comprometimento.

5.5.12. Deverá avaliar (testar, medir e aprimorar) uma ampla gama de controles de segurança em toda a infraestrutura da CMB, ajudando a identificar potenciais fraquezas e melhorar a postura geral de segurança, incluindo ao menos:

I. **Controles de rede:** Testar a eficácia dos controles relacionados ao Next-Generation Firewalls (NGFW), Intrusion Prevention Systems (IPS), Web Application Firewall (WAF) e segmentação de rede;

II. **Controles de endpoint:** Testar a eficácia das soluções antimalware, Host-based Intrusion Prevention Systems (HIPS), soluções Endpoint Detection and Response (EDR) e firewalls baseados em host;

III. **Controles de segurança de e-mail:** Testar a eficácia dos sistemas de filtragem de e-mail da organização, a segurança do gateway de e-mail, os filtros de spam e as medidas antiphishing;

IV. **Controles de vulnerabilidades:** Testar a eficácia do processo de gerenciamento de patches e vulnerabilidades, oferecendo insights

sobre a postura de segurança da organização, permitindo tratar riscos potenciais proativamente e fortalecer as defesas contra ameaças;

V. **Controles de segurança de dados:** Testar a eficácia de soluções de Prevenção de Perda de Dados (Data Loss Prevention - DLP), objetivando identificar potenciais fraquezas nos controles de proteção de dados para reduzir o risco de violações;

5.5.13. Deverá permitir a realização de simulações de ameaças do mundo real, o que poderá ocorrer de forma contínua (com opção de agendamento), não requerendo nenhuma interação humana, e sob demanda (acionamento manual), testando o ciclo de vida completo do ataque contra a infraestrutura da CMB, incluindo ao menos:

I. **Malware e Ransomware:** Simular o comportamento de várias infecções por malware e ransomware para testar a eficácia das soluções de proteção de endpoint, mecanismos de detecção de ameaças e capacidades de resposta a incidentes, incluindo malware de download (projetado para baixar e instalar software malicioso no sistema), wiper (malware destrutivo cuja principal função é apagar dados dos sistemas), infostealers (malwares projetados para roubar informações sensíveis do sistema) e backdoors (malwares que criam uma porta de entrada permitindo que os atacantes acessem e controlem o sistema remotamente);

II. **Ataques de credenciais:** Simular ataques que realizem bypass de autenticação a fim de validar a proteção de credenciais;

III. **Exploração de vulnerabilidades:** Simular a exploração de vulnerabilidades conhecidas e emergentes em softwares e sistemas operacionais, monitorando ativamente fontes como o banco de dados de CVE e novas descobertas para integrar os exploits mais recentes na biblioteca de ameaças;

IV. **Advanced Persistent Threat (APTs):** Simular ataques multiestágios usados por grupos APT para testar a capacidade da organização de detectar, responder e se recuperar de ameaças altamente direcionadas e sofisticadas, permitido desenvolver defesas direcionadas para proteger contra o cenário de ameaças em evolução representado pelos APTs. Terá o objetivo de revelar vulnerabilidades potenciais em segurança de rede e proteção de endpoint;

V. **Movimentação lateral:** Deve ser capaz de simular ataques de movimentação lateral entre os agentes instalados no ambiente a fim de verificar os controles de segurança internos implementados;

VI. **Exfiltração de dados:** Simular ataques que utilizem diferentes técnicas de exfiltração de dados.

5.5.14. Deverá classificar e informar o valor percentual das simulações executadas por nível de severidade (Ex. Alta, Média e Baixa);

5.5.15. Deverá ter seu portfólio de ataques baseado em frameworks de segurança cibernética, tais como: MITRE ATTACK, OWASP ou NIST;

5.5.16. Deverá mapear cada técnica de ataque dentro da estrutura MITRE ATTACK, permitindo simulações personalizáveis visando grupos de ameaças específicos e aumentando a precisão e a eficácia das avaliações de segurança;

5.5.17. Deverá possuir a instrumentação de IoCs provenientes de provedores de Threat Intelligence e/ou laboratório de inteligência de ameaça do fabricante da solução;

5.5.18. Deverá permitir a personalização de diferentes cenários de ataque, que se alinham com cenários de ameaças específico, apetite de risco e requisitos de conformidade da CMB, permitindo inclusive definir um escopo e quais ataques executar no teste;

5.5.19. Deverá possuir simulações de campanhas de ameaças, com link para o relatório da identificação e descrição da ameaça em campo, descrevendo seus impactos e identificando as regiões do mundo afetadas pela campanha;

5.5.20. Deverá permitir customização de simulação de campanhas de ameaças utilizando os seguintes IoCs: hash de arquivos, nome do host, URLs ou endereços IPv4;

5.5.21. Deverá simular ataques encadeados para validação de Cyber Kill Chain, ajudando a entender se os ativos estão protegidos e se as ameaças podem levar a violação ou perda de dados;

5.5.22. Deverá fazer uso de técnicas de Inteligência Artificial (IA) para auxiliar no processo de simulação dos ataques;

5.5.23. Deverá fornecer resultados e métricas em tempo real, incluindo uma pontuação geral de segurança da CMB, ajudando a medir o desempenho e comprovar o valor dos controles;

5.5.24. Deverá possuir dashboards e relatórios, além de viabilizar buscas interativas pelo sistema;

5.5.25. Todo o conjunto de funcionalidades exigidas para a solução tecnológica ofertada deverá operar de forma integrada e interoperável, sem prejuízo da flexibilidade prevista nos itens 1.34, 1.35 e 1.36.

5.6. SECURITY SERVICE EDGE (SSE)

5.6.1. A solução tecnológica ofertada, ou o conjunto de soluções integradas, deverá garantir o acesso seguro de usuários às aplicações/sistemas corporativos, além de proporcionar o controle da navegação Web, permitindo um gerenciamento centralizado das políticas. Para tanto, a solução deverá contemplar, no mínimo, as seguintes funcionalidades:

I. Zero Trust Network Access (ZTNA);

II. Firewall-as-a-Service (FWaaS);

III. Secure Web Gateway (SWG).

5.6.2. Deverá ter a capacidade de gerenciar o acesso de ao menos **200 (duzentos) usuários**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais usuários conforme sua preferência, desde que respeitado o limite estabelecido;

5.6.3. Deverá ser dotada de console de administração centralizada, contemplando uma interface gráfica (Graphical User Interface - GUI) acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.);

5.6.4. Deverá fazer uso de protocolos seguros para comunicação criptografada entre os diferentes componentes da solução, assim como para o acesso à sua console de administração;

5.6.5. Deverá permitir autenticação Single Sign-On (SSO) integrada com os serviços do Active Directory Domain Services (AD DS) ou com o Microsoft Entra ID, o que poderá ocorrer através de um ou mais protocolos padrão de mercado, tais como: RADIUS, LDAP, SAML, OAuth, Kerberos, etc;

5.6.6. Deverá permitir a habilitação de autenticação por multifator (Multi-Factor Authentication - MFA) de terceiros ou do próprio fabricante para gerenciamento da solução;

5.6.7. Deverá contar com Application Programming Interface (API) RESTful para permitir a integração eficiente com outras aplicações e serviços;

5.6.8. Deverá permitir que usuários recebam permissões específicas com base em suas funções (Role-Based Access Control - RBAC);

5.6.9. Deverá gerar e manter, pelo período mínimo de 30 (trinta) dias, o histórico completo de trilhas de auditoria que permita o rastreamento dos acessos executados por todos os usuários (logs);

5.6.10. Não poderá apresentar limitação quanto ao número de acessos simultâneas autorizados a administrar a solução, desde que devidamente licenciados;

5.6.11. Deverá contar com distintos pontos de presença (Point of Presence - PoP), espalhados em diversos continentes (Américas, Europa África e Ásia), a fim de garantir uma boa performance e experiência para os usuários de acordo com a sua localização;

5.6.11.1. Deve contar com ao menos 2 (dois) pontos de presença no Brasil para tratamento e encaminhamento do tráfego nacional;

5.6.11.2. A inspeção do conteúdo de conexões originadas no Brasil, envolvendo todas as funcionalidades de segurança solicitadas, deve ser feita em datacenter dentro do território brasileiro, sem a necessidade de desvio do tráfego ou saída para outros países (exceto para usuários que estiverem fora do território nacional ou devido a falha nos pontos de presença);

5.6.11.3. Deve ter a capacidade de automaticamente determinar e estabelecer conexões com pontos de presença de menor latência, garantindo uma boa performance para os usuários.

5.6.12. Deverá ser compatível para utilização em qualquer tipo de dispositivo (corporativo ou pessoal), fazendo ou não o uso de “agente” instalado no sistema operacional, independentes de estarem localizados dentro ou fora da organização;

5.6.12.1. Quando fizer uso de agente instalado no dispositivo, todas as funcionalidades exigidas neste Termo de Referência devem estar funcionais para o usuário;

5.6.12.2. Quando NÃO fizer uso de agente instalado no dispositivo (agentless), deve permitir os acessos às aplicações corporativas via portal Web disponibilizado através da própria solução, suportando ao menos os protocolos HTTP/HTTPS, RDP e SSH;

5.6.12.3. O agente deve ser compatível ao menos com as seguintes versões de sistemas operacionais:

I. Windows 10 ou superior;
II. MacOS 13 ou superior;
III. Android 12 ou superior;
IV. iOS 15 ou superior.

5.6.12.4. O agente deve ter a capacidade de estabelecer um túnel criptografado entre o dispositivo do usuário e a nuvem da solução, garantido que todo tráfego do usuário seja inspecionado e tratado conforme as políticas estabelecidas;

5.6.12.5. Deve permitir a definição de quais redes podem ser roteadas para dentro do túnel criptografado estabelecido com a solução (split tunneling);

5.6.12.6. Deve permitir o gerenciamento dos agentes pela console de administração da solução, possibilitando a aplicação das configurações e políticas de modo centralizado;

5.6.12.7. Deve permitir configuração de encaminhamento do tráfego adaptável, conforme a localização do dispositivo, permitindo a sua identificação quando estiver dentro ou fora da empresa;

5.6.12.8. Deve permitir a proteção contra desativação do agente instalado, através do uso de uma senha definida pelo administrador;

5.6.12.9. Deve permitir o envio de e-mail, através da console de administração, para usuários diversos, contendo o link para download do agente a ser instalado na estação;

5.6.12.10. Deve permitir a inicialização automática do agente em conjunto com a inicialização do sistema operacional;

5.6.12.11. Deve permitir a definição da ativação ou desativação de atualizações automáticas do agente instalado;

5.6.12.12. O agente deve ter a capacidade de realizar conexão automática transparente (sem intervenção do usuário) com a nuvem da solução, além de negar qualquer acesso ao usuário em caso de perda de comunicação do agente;

5.6.13. Deverá criar inventário contendo todos os dispositivos conectados à solução. O inventário deverá conter minimamente as seguintes informações:

I. Usuário conectado no dispositivo;
II. Nome do dispositivo;
III. Tipo de dispositivo;

IV. Nome e versão do sistema operacional;

V. Conformidade da postura de segurança do dispositivo.

5.6.14. Deverá implementar uma arquitetura Zero Trust, permitindo a definição de uma política granular que garanta o acesso de menor privilégio aos aplicativos/sistemas corporativos, concedido exclusivamente às pessoas autorizadas;

5.6.14.1. Os usuários não devem ter visibilidade de aplicativos não autorizados. Caso um usuário obtenha o endereço de acesso (URL) para uma determinada aplicação, no qual ele não tem permissão, o acesso deve ser bloqueado pela solução;

5.6.14.2. Todo usuário que tentar acessar um aplicativo corporativo deve, primeiramente, ser autenticado e autorizado pelos provedores de identidade previamente configurados.

5.6.15. Com o objetivo de viabilizar o acesso remoto seguro dos usuários às aplicações e aos sistemas corporativos internos da CMB, bem como assegurar que todo o tráfego de saída de uma determinada localidade seja encaminhado e inspecionado pela solução ofertada, a CONTRATADA poderá adotar uma das seguintes arquiteturas:

I. Implementação de serviço de Conector/Gateway no ambiente de virtualização da CMB, obrigatoriamente compatível com o hypervisor VMware, operando em arquitetura de alta disponibilidade (High Availability – HA), composta por, no mínimo, 2 (dois) nós redundantes;

OU

II. Estabelecimento de conexão segura entre o ambiente da CMB e a nuvem da solução, podendo ser implementada por intermédio do NGFW corporativo da própria CMB ou por equipamentos especializados de SD-WAN, fornecidos, implementados e gerenciados pela CONTRATADA. Quando adotada a utilização de equipamentos de SD-WAN, estes deverão operar em arquitetura de alta disponibilidade (High Availability – HA), composta por, no mínimo, 2 (dois) nós redundantes.

5.6.16. No caso da utilização do serviço de “conector/gateway”, deverão ser observadas as seguintes condições:

I. O serviço necessário ao seu funcionamento deverá ser compatível para instalação em servidor com sistema operacional Linux ou

Windows, a ser fornecido e instalado pela própria CMB, cabendo à CONTRATADA prestar as devidas orientações para a sua correta configuração e funcionamento;

II. No caso do sistema operacional Windows, o servidor fornecido pela CMB será disponibilizado apenas com as licenças Windows Server Datacenter e CAL (Client Access License), cabendo à CONTRATADA o fornecimento de todas as demais licenças necessárias para o correto funcionamento do serviço;

III. Deverá ser instalado atrás do firewall da CMB, em rede de sua conveniência, de acordo com as recomendações do fabricante;

IV. A CMB ficará responsável pelo seu backup e recuperação em caso de eventual incidente que leve a sua indisponibilidade, cabendo ainda à CONTRATADA prestar todo o apoio necessário para viabilizar esse processo.

5.6.17. Deverá permitir a criação de políticas para avaliar a postura dos dispositivos (status de segurança), visando garantir que apenas dispositivos que atendem as condições de segurança especificadas pelo administrador possam acessar as aplicações/sistemas. Ao menos os seguintes tipos de política de postura devem ser suportados:

I. Para Sistemas Windows:

- Verificação da presença de antivírus instalado;
- Verificação da presença de um arquivo específico;
- Verificação de um certificado específico instalado
- Verificação de um processo específico em execução;
- Verificação de uma chave de registro específica;
- Verificação se associação ao Active Directory;
- Verificação da versão do sistema operacional da instalado.

II. Para Sistemas MacOS:

- Verificação da presença de antivírus instalado;
- Verificação da presença de um arquivo específico;
- Verificação de um processo específico em execução;
- Verificação de um certificado específico instalado;
- Verificação da versão do sistema operacional da estação;

III. Para Sistemas Linux:

- Verificação da presença de antivírus instalado;

- Verificação da presença de um arquivo específico;
- Verificação de um processo específico em execução.

5.6.18. Deverá permitir a criação de políticas de firewall baseado em nuvem visando garantir a segurança do tráfego de saída para diferentes portas e protocolos;

5.6.18.1. Deve permitir a criação de políticas tradicionais baseado em endereços IP de origem/destino, portas de origem/destino e protocolo (TCP, UDP, etc.);

5.6.18.2. Deve permitir a criação de políticas com base em usuários individuais ou grupos de usuários, integrando-se com o provedor de identidade utilizado;

5.6.18.3. Deve permitir a criação de políticas usando Fully Qualified Domain Name (FQDNs) e curingas (wildcards) para abranger múltiplos subdomínios;

5.6.18.4. Deve registrar todos os eventos, fornecendo logs detalhados para auditoria, conformidade, análise de segurança e solução de problemas.

5.6.19. Deverá permitir a realização de um controle abrangente e flexível sobre a navegação Web dos usuários, garantindo que a CMB possa proteger seus usuários e dados, cumprir políticas e otimizar o uso do serviço de internet corporativo;

5.6.19.1. Deve permitir a criação de políticas para o controle da navegação Web dos usuários, possibilitando consentir ou bloquear o acesso a URL’s ou categorias específicas, de acordo com regras definidas para grupos de usuários determinados;

5.6.19.2. Deve contar nativamente com, no mínimo, 70 (setenta) categorias distintas de páginas Web que poderão ser utilizadas para criação das políticas, além de permitir a criação de categorias customizadas;

5.6.19.3. Deve permitir a aplicação de restrições de acesso por períodos específicos (dia e horário), conforme a necessidade da organização;

5.6.19.4. Deve possuir ferramenta de consulta de sites para permitir que os administradores consultem a categoria de um site específico (site lookup tool);

5.6.19.5. Deve permitir que os administradores possam solicitar uma reclassificação caso um site esteja incorretamente categorizado, garantindo a precisão das políticas;

5.6.19.6. Deve permitir a criação de regras específicas de exceção (bypass), possibilitando que determinadas categorias ou domínios não passem pela inspeção de segurança;

5.6.19.7. Em caso de bloqueio da navegação, o usuário deve ser direcionado para uma página de bloqueio da própria solução;

5.6.19.8. Deve ser capaz de inspecionar todo o tráfego criptografado de navegação (HTTPS);

5.6.20. Deverá realizar a inspeção dos arquivos trafegados pelos usuários durante a navegação, aplicando defesa robusta contra uma ampla gama de ameaças cibernéticas, através da combinação de tecnologias avançadas como aprendizado de máquina, inteligência de ameaças e sandboxing;

5.6.20.1. Deve possuir mecanismos para identificação e bloqueio de malware, ransomware e Advanced Persistent Threat (APT);

5.6.20.2. O fabricante da solução deve fazer uso de diferentes fontes de inteligência de ameaças (Threat Intelligence) para detecção de ameaças;

5.6.20.3. Deve fazer uso de Machine Learning (ML) para Análise de Arquivos Executáveis Portáteis (PE) visando a detecção e bloqueio de Malwares desconhecidos (Zero Day), além de identificar domínios de Phishing (páginas falsas que tentam roubar informações), bloqueando o acesso a esses sites;

5.6.20.4. Deve fazer uso de Sandboxing para confirmar as detecções feitas pelos mecanismos antimalware e de Machine Learning.

5.6.21. Deverá possuir dashboards e relatórios nativos, além de viabilizar buscas interativas de informações pelo sistema:

5.6.22. Todo o conjunto de funcionalidades exigidas para a solução tecnológica ofertada deverá operar de forma integrada e interoperável, sem prejuízo da flexibilidade prevista nos itens 1.34, 1.35 e 1.36.

5.7. WEB APPLICATION SECURITY PLATFORM

5.7.1. A solução tecnológica ofertada, ou o conjunto de soluções integradas, deverá garantir a continuidade e segurança dos serviços Web da CMB, independentemente de onde estejam hospedados (on-premise, multinuvem ou híbrido). Para tanto, a solução deverá contemplar, no mínimo, as seguintes funcionalidades:

I. Global Server Load Balancing (GSLB);
II. Authoritative DNS com DNSSEC;
III. Web Application and API Protection (WAAP).

5.7.2. Deverá ter a capacidade de balancear o tráfego para ao menos **2 (dois) sites distintos (localidades)** e **20 (vinte) aplicações**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais localidades e aplicações conforme sua preferência, desde que respeitado o limite estabelecido;

5.7.3. Deverá ter a capacidade de cadastrar ao menos **4 (quatro) domínios (zonas)** no serviço de DNS autoritativo, sem limite de resoluções e resposta, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais domínios conforme sua preferência, desde que respeitado o limite estabelecido;

5.7.4. Deverá ter a capacidade de monitorar ao menos **500 GB (quinhentos gigabytes) de tráfego mensal** direcionado aos serviços Web e APIs da CMB, possibilitando que CMB tenha a flexibilidade de adicionar, remover ou substituir tais serviços conforme sua preferência, desde que respeitado o limite estabelecido;

5.7.4.1. Para fins de contabilização do tráfego, deverá ser considerado apenas o “tráfego legítimo” (limpo), sendo vedada a inclusão de qualquer volume de dados associado a tentativas de ataque ou tráfego malicioso que tenha sido detectado e bloqueado pela solução.

5.7.5. Deverá ter a capacidade de realizar a descoberta de API’s para ao menos **10 (dez) aplicações**, possibilitando que a CMB tenha a flexibilidade de adicionar, remover ou substituir tais aplicações conforme sua preferência, desde que respeitado o limite estabelecido;

5.7.5.1. Entende-se por aplicações como a configuração de um FQDN ou domínio que deve ser protegido por uma política de segurança, acessível por um IP ou CNAME, independentemente da quantidade de paths ou URL deste FQDN.

5.7.6. Deverá ser dotada de console de administração centralizada, contemplando uma interface gráfica (Graphical User Interface - GUI) acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.);

5.7.7. Deverá fazer uso de protocolos seguros para comunicação criptografada entre os diferentes componentes da solução, assim como para o acesso à sua console de administração;

5.7.8. Deverá contar com Application Programming Interface (API) RESTful para permitir a integração eficiente com outras aplicações e serviços;

5.7.9. Deverá permitir autenticação Single Sign-On (SSO) integrada com os serviços do Active Directory Domain Services (AD DS) ou com o Microsoft Entra ID, o que poderá ocorrer através de um ou mais protocolos padrão de mercado, tais como: RADIUS, LDAP, SAML, OAuth, Kerberos, etc;

5.7.10. Deverá permitir a habilitação de autenticação por multifator (Multi-Factor Authentication - MFA) de terceiros ou do próprio fabricante para gerenciamento da solução;

5.7.11. Deverá permitir que usuários recebam permissões específicas com base em suas funções (Role-Based Access Control - RBAC);

5.7.12. Deverá gerar e manter, pelo período mínimo de 30 (trinta) dias, o histórico completo de trilhas de auditoria que permita o rastreamento dos acessos executados por todos os usuários (logs);

5.7.13. Não poderá apresentar limitação quanto ao número de acessos simultâneas autorizados a administrar a solução, desde que devidamente licenciados;

5.7.14. O fabricante da solução deverá contar com rede de inteligência de ameaças (Threat Intelligence) para aprimoramento dos seus controles de segurança;

5.7.15. Deverá permitir a criação de políticas específicas voltadas para a distribuição/balanceamento do tráfego, tomando como base as condições estabelecidas pelo administrador. Ao menos os seguintes algoritmos/lógicas de distribuição de carga devem estar presentes na solução:

I. **Ativo-passivo Failover:** distribui o tráfego para o data center primário/principal até que as condições de falha configuradas sejam atingidas, redirecionando automaticamente o tráfego para o data center passivo/backup;

II. **Ativo-Ativo Failover:** distribui tráfego aleatoriamente entre dois ou mais data centers até que algum deles atinja as condições de falha configuradas, possibilitando inclusive a definição de pesos diferentes para cada data center;

III. **Localização geográfica:** distribui tráfego com base na localização (região) do cliente, direcionando-o para o data center mais próximo.

5.7.16. Deverá monitorar a disponibilidade e integridade das aplicações para a distribuição/balanceamento, capturando as condições de tráfego em relação aos data centers onde os serviços encontram-se hospedados;

5.7.16.1. Deve oferecer suporte para ao menos os seguintes protocolos para monitoramento: HTTP, HTTPS e TCP;

5.7.16.2. Deve permitir a definição do número da porta específica que deverá ser utilizada para o monitoramento;

5.7.16.3. Deve permitir a especificação da frequência com que os testes deverão ser executados e o tempo limite de espera (timeout) da resposta para identificação da falha;

5.7.16.4. Deve contar com mecanismos para identificar quanto um determinado destino do balanceamento estiver apresentando intermitência no seu funcionando, deixando de distribuir tráfego para mesmo até que seja considerado estável;

5.7.16.5. Deve permitir a definição de cabeçalho HTTP/HTTPS específico a ser usando para o monitoramento.

5.7.17. Para funcionamento das suas funcionalidades, a solução deverá possuir pontos de presença (Point of Presence - PoP) distribuídos em diferentes regiões globais na internet;

5.7.17.1. Visando garantir uma melhor performance aos serviços, a solução deverá contar obrigatoriamente com ao menos 1 (um) pontos de presença no Brasil.

5.7.18. Deverá permitir a inclusão de certificados SSL/TLS próprios da CMB para a conexão à sua infraestrutura, emitidos por Autoridade Certificadora (AC) de sua preferência, dando ao administrador a possibilidade de importar a cadeia certificadora para a solução;

5.7.18.1. O compartilhamento e armazenamento de chaves deve ocorrer de acordo com processos e tecnologias que sigam um padrão internacional reconhecidamente aceito e que não exponham as chaves em texto-claro;

5.7.18.2. Deve permitir o uso do protocolo TLS 1.2 ou superior, possibilitando que a CMB possa configurar as cifras para cada URL monitorada, suportando ao menos:

tls_ecdhe_ecdsa_with_aes_128_gcm_sha256

tls_ecdhe_ecdsa_with_aes_256_gcm_sha384
tls_ecdhe_rsa_with_aes_128_gcm_sha256
tls_ecdhe_rsa_with_aes_256_gcm_sha384

5.7.18.3. Os Certificados Digitais A1 SSL/TLS poderão ser individualizados para cada URL implantada ou do tipo SAN (Subject Alternative Name), onde um único certificado pode conter várias URL conforme definição da CMB;

5.7.18.4. Quando da necessidade de validação do cliente por meio de certificado digital (mTLS, por exemplo) deverão ser feitas as validações previstas no método X509_verify_cert, existente na estrutura do Openssl.

5.7.19. Deverá oferecer serviço de DNS autoritativo completo, incluindo DNSSec (Domain Name System Security Extensions) para permitir a assinatura digital dos dados da zona, evitando ataques de envenenamento de cache DNS e sequestro de DNS;

5.7.19.1. Deve permitir a implementação de zonas primárias ou secundárias, substituindo ou aumentando a infraestrutura DNS da CMB;

5.7.19.2. Deve permitir a criação, alteração e exclusão dos seguintes tipos de records DNS: SOA, A/AAAA, CNAME, NS, MX, TXT, SRV, SPF e PTR;

5.7.19.3. Deve permitir a criação, alteração e exclusão dos seguintes tipos de records DNSSec: DNSKEY, RRSIG, DS e NSEC3;

5.7.19.4. Deve autogerenciar a assinatura da zona do DNSSec, realizando a rotação automática da Zone-Signing Keys (ZSK) e Key Signing Key (KSK). As chaves ZSK e o KSK deverão ser rotacionadas, antes da sua expiração, em uma periodicidade mínima semanal e anual, respectivamente.

5.7.19.5. Deve contar com uma infraestrutura altamente escalonável com capacidade suficiente para absorver ataques de DDoS e, ao mesmo tempo, atender solicitações legítimas;

5.7.19.6. Deve possuir ao menos 01 (um) ponto de presença para resolução de DNS localizado no Brasil;

5.7.19.7. Deve mitigar, no mínimo, os seguintes tipos de ataques de DDoS: esgotamento de recursos (NXDOMAIN, PRSD, DNS flood, etc,), consultas diretas, falsificação do IP de origem e ataques de TTL (Time to Live).

5.7.20. Deverá oferecer mecanismo de proteção para aplicativos Web e APIs (WAAP) que permita monitorar, filtrar e bloquear de forma eficaz o tráfego HTTP/S malicioso;

5.7.20.1. Deve fazer o uso de machine learning para detectar anomalias e bloquear ataques em tempo real, identificando vazamento/adulteração de dados, violações de políticas, comportamento suspeito e ataques relacionados a todos os riscos de segurança listados no OWASP TOP 10 Web Application Security Risks;

5.7.20.2. Deve possuir políticas nativas para filtragem de tráfego, além de permitir a customização de novas, possibilitando o seu gerenciamento de forma agrupada ou individual;

5.7.20.3. Deve permitir a atribuição de políticas para segmentos específicos da URL que está atrelada ao aplicativo Web e API protegido;

5.7.20.4. Deve permitir a criação de políticas de forma passiva (monitor only), possibilitando visualizar (por meio de alertas) o seu comportamento antes da sua ativação efetiva no ambiente;

5.7.20.5. Deve tratar de maneira individualizada as requisições maliciosas direcionadas aos aplicativos Web e API;

5.7.20.6. Deve permitir a criação de políticas de bloqueio ou permissão do tráfego com base no endereço IP, sub-rede (CIDR) e área geográfica específica;

5.7.20.7. Deve implementar análise do tráfego para proteger não só contra vários vetores de ataque conhecidos (assinatura), mas também de comportamentos suspeitos;

5.7.20.8. Deve permitir o bloqueio de ataques no modo blacklisting e whitelisting;

5.7.20.9. Deve possuir funcionalidade de aprendizagem automática do funcionamento de uma aplicação Web (URLs, parâmetros, campos de formulário, cookies, dentre outras) para a configuração de bloqueio por whitelisting;

5.7.20.10. Deve permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos já existentes, antes do seu envio à aplicação Web e API de destino;

5.7.20.11. Deve permitir a inclusão do IP original do cliente no campo X-Forwarded-For do cabeçalho HTTP;

5.7.20.12. Deve realizar inspeção completa do corpo das requisições HTML, com suporte mínimo de 32k;

5.7.20.13. Deve permitir a configuração da descoberta de API para identificar “Shadow API”, ou seja, API que foram expostas, mas não foram aprovadas, permitindo implementar políticas de controle da API a partir da descoberta;

5.7.20.14. Deve identificar API’s zumbis, ou seja, que foram descobertas, mas não possuem atividade ou tráfego;

5.7.20.15. Deve reduzir a superfície de ataque de APIs através da descoberta de API ocultas (Shadow APIs), identificando no mínimo, as seguintes informações: Nome do host, Caminho base, Caminho do recurso, Métodos, códigos de resposta, formato (JSON ou XML), quantidade de acessos, quantidade de erros apresentados (status 4XX e 5XX) e porcentual de clientes com má reputação que solicitaram a API;

5.7.20.16. Deve ter a capacidade de aplicar regras de WAF automáticas para proteção a ameaças emergentes (Zero Day).

5.7.21. Deverá detectar e diferenciar os acessos legítimos realizados por usuários humanos, dos acessos realizados por bots (maliciosos ou não) nos aplicativos Web e API’s da CMB, permitindo categorizá-los e mitigá-los com base no seu comportamento e características;

5.7.21.1. Deve detectar bots automaticamente fazendo o uso de base de bots conhecidos, aplicando modelos e técnicas de machine learning para análise do usuário, detecção de anomalias HTTP, detecção de navegador e altas taxas de solicitação;

5.7.21.2. Deve ter inteligência de aprendizado, incluindo uso de modelos de aprendizado de máquina (machine learning), para aplicar corretamente as assinaturas de defesa evitando causar falsos positivos. Estas ações deverão ser feitas a partir do aprendizado automatizado de tráfego legítimo e sem a interferência manual de configurações;

5.7.21.3. Deve prover defesa proativa contra bots por meio da injeção de um desafio JavaScript para detectar se é um usuário legítimo;

5.7.21.4. Deve permitir a criação de políticas de forma passiva (monitor only), permitido visualizar (por meio de alertas) o seu comportamento antes da sua ativação;

5.7.21.5. Deve detectar e bloquear o uso de search crawlers e scanners de vulnerabilidade;

5.7.21.6. Deve possuir políticas nativas para tratamento dos bots, além de permitir a customização de novas, possibilitando ao menos as seguintes ações: Permitir o acesso, bloquear o acesso e retornar código de erro HTTP 403 (acesso negado), bloquear o acesso e retornar com mensagem customizada;

5.7.21.7. Deve contar com uma base nativa de bots conhecidos separados por categoria, mantendo-a atualizada periodicamente, permitindo a criação de políticas com base nessas categorias. Deve permitir ainda a criação de categorias pelo administrador, vinculando bots específicos dentro de cada categoria criada;

5.7.21.8. Deve ter a capacidade de validar se a conexão realizada foi feita por um bot através de Captcha criptográfico, sem a intervenção do usuário;

5.7.21.9. Deve ter a capacidade de validar se a conexão foi feita por um bot através de validação ativa do navegador, através da execução de JavaScript e armazenamento de Cookies (Interstitial Challenge).

5.7.22. Deverá bloquear ataques de Distributed Denial of Service (DDoS) de camada 7 (modelo OSI), com o objetivo de proteger as aplicações Web e APIs, de forma a assegurar a continuidade dos serviços da CMB;

5.7.22.1. Deve prover serviço de defesa aos ataques no perímetro da rede (EDGE) da solução, evitando que estes alcancem as aplicações Web e APIs;

5.7.22.2. Deve mitigar ataques de forma transparente, absorvendo e bloqueando ataques de TCP SYN flood, UDP Floods e ICMP floods, HTTP floods, IP spoofing e Slowloris,

5.7.22.3. Deve possuir proteção por meio de controles de taxa (rate limit), tanto para ataques que enviam solicitações a uma taxa excessiva,

quanto para ataques com taxas de solicitação extremamente lentas, permitindo designação de um limite aceitável.

5.7.23. Deverá possuir "alertas" pré-definidos nativamente na solução, possibilitando inclusive o seu envio automático por e-mail;

5.7.24. Deverá permitir a criação e customização de dashboards e relatórios, além de viabilizar buscas interativas de informações pelo sistema;

5.7.25. Todo o conjunto de funcionalidades exigidas para a solução tecnológica ofertada deverá operar de forma integrada e interoperável, sem prejuízo da flexibilidade prevista nos itens 1.34, 1.35 e 1.36.

5.8. UNIFIED IDENTITY SECURITY PLATFORM

5.8.1. A solução tecnológica ofertada, ou o conjunto de soluções integradas, deverá assegurar o controle, a rastreabilidade e a auditoria das identidades e segredos utilizados pelos usuários para acesso aos recursos da CMB. Para tanto, a solução deverá contemplar, no mínimo, as seguintes funcionalidades:

I. Privileged Access Management (PAM);
II. Vendor Privileged Access Manager (VPAM);
III. Secrets Management;
IV. Endpoint Privilege Management (EPM);
V. Personal Vault.

5.8.2. Deverá ter a capacidade de gerenciar o acesso de ao menos **40 (quarenta) usuários privilegiados (PAM)**, **10 (dez) usuários de fornecedores (VPAM)** e **50 (cinquenta) servidores de aplicação (Secrets Management)** OU possibilitar o acesso de ao menos **100 (cem) usuários conectados na plataforma**, permitindo que a CMB tenha a flexibilidade de atribuir tais licenças conforme sua preferência, desde que respeitado o limite estabelecido;

5.8.3. Deverá ter a capacidade de gerenciar usuários locais (EPM) presentes em ao menos **1500 (mil e quinhentos) de desktops Windows** e **410 (quatrocentos e dez) servidores (sendo 200 Windows e 210 Linux)**, permitindo que a CMB tenha a flexibilidade de atribuir tais licenças conforme sua preferência, desde que respeitado o limite estabelecido;

5.8.4. Deverá ter a capacidade de fornecer cofre pessoal de senhas (Personal Vault) para ao menos **1000 (mil) usuários,** permitindo que a CMB tenha a

flexibilidade de atribuir tais licenças conforme sua preferência, desde que respeitado o limite estabelecido;

5.8.5. Deverá ser dotada de console de administração centralizada, contemplando uma interface gráfica (Graphical User Interface - GUI) acessível via navegador Web padrão (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.);

5.8.6. Deverá fazer uso de protocolos seguros para comunicação criptografada entre os diferentes componentes da solução, assim como para o acesso à sua console de administração;

5.8.7. Deverá contar com Application Programming Interface (API) RESTful para permitir a integração eficiente com outras aplicações e serviços;

5.8.8. Deverá permitir autenticação Single Sign-On (SSO) integrada com os serviços do Active Directory Domain Services (AD DS) ou com o Microsoft Entra ID, o que poderá ocorrer através de um ou mais protocolos padrão de mercado, tais como: RADIUS, LDAP, SAML, OAuth, Kerberos, etc;

5.8.9. Deverá permitir a habilitação de autenticação por multifator (Multi-Factor Authentication - MFA) de terceiros ou do próprio fabricante para gerenciamento da solução;

5.8.10. Permitir que usuários recebam permissões específicas com base em suas funções (Role-Based Access Control - RBAC);

5.8.11. Deverá gerar e manter, pelo período mínimo de 30 (trinta) dias, o histórico completo de trilhas de auditoria que permita o rastreamento dos acessos executados por todos os usuários (logs);

5.8.12. Não poderá apresentar limitação quanto ao número de acessos simultâneas autorizados a administrar a solução, desde que devidamente licenciados;

5.8.13. O fabricante da solução deverá contar com rede de inteligência de ameaças (Threat Intelligence) para aprimoramento dos seus controles de segurança;

5.8.14. Deverá detectar comportamentos anormais (ações que possam representar riscos), além de monitorar, gravar e auditar as sessões realizadas pelos usuários da solução nos sistemas-alvo presentes no ambiente tecnológico da CMB;

5.8.14.1. Um sistema-alvo pode ser entendido como um servidor, estação de trabalho, ativo de rede/segurança, dentre outros, cujas credenciais de acesso passem a ser protegidas e gerenciadas pela solução

ofertada. Ao menos os seguintes tipos de contas deverão ser suportados:

I. Contas de sistemas operacionais Linux e Microsoft Windows (on-premise ou cloud);
II. Contas em plataformas Hypervisor (mínimo VMWare);
III. Contas de sistemas e de serviço (não humanos);
IV. Contas de usuários e administradores de bancos de dados Microsoft SQL Server e PostgreSQL;
V. Contas de ativos de rede, tal como: switches, roteadores, controladoras e Access Point (AP) Wi-Fi e NAS (Network Attached Storage);
VI. Contas de ativos de segurança (equipamentos dedicados à segurança);
VII. Contas de fornecedores terceirizados.

5.8.14.2. Um usuário da solução pode ser entendido como qualquer pessoa que acesse um sistema-alvo mediante logon na solução e faça uso de credenciais por ela gerenciada.

5.8.15. Os comandos e vídeos das sessões gravadas devem ser indexados para pesquisas futuras, possibilitando inclusive o uso de filtros para buscar comandos e ações executadas ao longo da sessão;

5.8.15.1. Os comandos e os vídeos devem ser gravados em formato padrão de mercado (não proprietário);

5.8.15.2. Deve ser permitido a definição de um período de retenção máximo para os vídeos das sessões gravadas.

5.8.16. Deverá permitir o acesso remoto seguro de usuários simultâneos nos sistemas-alvo, em conformidade com quantitativo de licenças solicitado, sem a necessidade de instalação e uso de quaisquer softwares clientes/agente nos dispositivos;

5.8.16.1. Deve permitir o acesso aos sistema-alvo utilizando “Remote Desktop” e “SSH” (desde que tecnicamente compatível), possibilitando que os usuários façam o acesso sem a necessidade de realizar login interativo prévio no sistema operacional e conhecer a senha/chave atualmente vigente no sistema-alvo;

5.8.16.2. Deve ter a capacidade de recuperar do seu cofre de senhas (vault), de forma automática e transparente, as credenciais necessárias para

viabilizar a conexão remota, bastando que o usuário acesse o sistema-alvo desejado através de um portal Web devidamente autenticado com usuário e senha pré-determinados ou recuperados da base de dados da solução.

5.8.17. Deverá possibilitar que o administrador possa permitir ou não a transferência de arquivos entre a estação de trabalho local do usuário e o sistema-alvo acessado remotamente;

5.8.18. Deverá identificar e correlacionar ações que caracterizam abusos, comportamentos anormais e fora dos padrões aprendidos/mapeados, devendo montar perfis de comportamento gerais dos acessos;

5.8.19. Deverá proteger os sistemas-alvo contra a perda, roubo e gestão inadequada de credenciais (contas locais e do Active Directory), permitindo a definição de regras para quantidade de caracteres, frequência de troca automatizada e especificação de caracteres permitidos ou proibidos na composição da senha (complexidade);

5.8.20. Deverá possuir recurso para realizar a descoberta de credenciais privilegiadas presentes nos dispositivos conectados na rede corporativa, possibilitando inclusive a importação das credenciais descobertas para a solução, viabilizando o seu gerenciamento;

5.8.20.1. Deve ser capaz de se conectar-se aos dispositivos da rede por meio de seus protocolos padrão, sem a necessidade da instalação um agente local;

5.8.20.2. Ao menos os seguintes tipos de contas privilegiadas devem ser descobertos pela solução: contas de domínio do Windows, contas locais (Windows e Linux) e chaves SSH;

5.8.20.3. Deve permitir a execução de varreduras de credenciais de forma manual ou automática (agendas recorrentes).

5.8.21. Deverá proteger as credenciais administrativas em um cofre de senhas seguro, permitindo a aplicação de políticas granulares de rotações e trocas automáticas das senhas, trilha de auditoria dos acessos, mitigando situações de roubo, perda e exploração de credenciais;

5.8.22. Deverá possuir funcionalidade para integração de servidores Linux ao Active Directory, mantendo a nomenclatura e estrutura de grupos do diretório. As contas e grupos do Active Directory com permissão de acesso devem ser provisionados de forma automatizada e transparente nos servidores Linux;

5.8.23. Deverá permitir a definição de Fluxos de Aprovação (Workflows) para obtenção dos acessos, apresentando ao menos as seguintes características:

I. Permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, para ao menos um responsável;

II. Permitir a aprovação perante um agendamento de ações administrativas, ou seja, a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos.

5.8.24. Deverá incorporar medidas de segurança como Certificação Common Criteria (CC) – ISO/IEC 15408 – para garantia de segurança do método utilizado no desenvolvimento do sistema de repositório seguro de credenciais e criptografia dos módulos da solução, a fim de proteger a informação em trânsito entre módulos da solução e aplicações Web dos usuários finais;

5.8.25. Deverá utilizar criptografia para armazenar as credenciais gerenciadas, aplicando algoritmos de criptografia hierárquica multicamadas compatíveis com FIPS 140-2 (Federal Information Processing Standard) para proteger os dados;

5.8.26. Para que os usuários remotos consigam se comunicar de forma segura com os sistemas-alvo, será permitido, caso necessário, a instalação de serviço de “conector/gateway” dentro do ambiente de virtualização da CMB (compatível obrigatoriamente com Hypervisor VMWare), atendendo as seguintes condições:

I. O serviço necessário ao seu funcionamento deverá ser compatível para instalação em servidor com sistema operacional Linux ou Windows, a ser fornecido e instalado pela própria CMB, cabendo à CONTRATADA prestar as devidas orientações para a sua correta configuração e funcionamento;

II. No caso do sistema operacional Windows, o servidor fornecido pela CMB será disponibilizado apenas com as licenças Windows Server Datacenter e CAL (Client Access License), cabendo à CONTRATADA o fornecimento de todas as demais licenças necessárias para o correto funcionamento do serviço;

III. Deverá ser instalado atrás do firewall da CMB, em rede de sua conveniência, de acordo com as recomendações do fabricante;

IV. A CMB ficará responsável pelo seu backup e recuperação em caso de eventual incidente que leve a sua indisponibilidade, cabendo ainda à CONTRATADA prestar todo o apoio necessário para viabilizar esse processo.

5.8.27. No caso da utilização de um servidor de “conector/gateway”, este deverá ser implementado em arquitetura de alta disponibilidade (High Availability – HA), respeitado o mínimo de 2 (dois) nós redundantes, possibilitando que o serviço continue funcionando mesmo em caso de indisponibilidade ou manutenção do servidor;

5.8.28. A solução deverá permitir o acesso remoto seguro de fornecedores terceirizados que precisam acessar sistemas-alvo da CMB, dando visibilidade e controle completos das atividades executadas, sem a necessidade da utilização de VPN ou agentes instalados;

5.8.28.1. Deve permitir o envio de “convites” por email aos fornecedores cadastrados, devendo conter todas as informações necessárias para orientá-los no procedimento para o acesso remoto, possibilitando inclusive a criação de modelos de “convites” personalizados;

5.8.28.2. Para o cadastro de fornecedores, deve permitir ao menos a inserção das seguintes informações: nome da empresa, nome do fornecedor e endereço de email;

5.8.28.3. Deve permitir a definição de um prazo de expiração para o cadastro dos fornecedores, carecendo do envio de um novo “convite” para permitir novamente o seu acesso;

5.8.28.4. Deve permitir a definição de um prazo de expiração dos “convites” enviados, tornando-os inválidos após esse período;

5.8.28.5. Deve apresentar compatibilidade, para viabilizar o acesso remoto, com pelo menos um dos seguintes métodos de autenticação: aplicativo para dispositivos móveis do tipo IOS e Android (com suporte para FaceID e leitor de digital) ou tokens OATH OTP via e-mail;

5.8.28.6. Deve permitir a definição de um período para limitar os acessos dos fornecedores, tais como: intervalo de datas permitidas, dias da semana permitidos e intervalo de horas permitidas. Além disso,

alinhado à definição deste período de acesso, deve possibilitar que seja definido um “Time Zone” distinto para cada fornecedor;

5.8.28.7. Deve permitir a definição de um intervalo de IP ou sub-rede de onde os usuários remotos poderão realizar os acessos.

5.8.29. A solução deverá armazenar, proteger e rotacionar credenciais (secrets) através de um repositório seguro (cofre de senhas), eliminando a necessidade manter credenciais estáticas diretamente no código-fonte, em scripts ou em arquivos de configuração (prática conhecida como hard-coded);

5.8.29.1. Deve fornecer controles de segurança adequados para acesso e proteção das credenciais, tais como: autenticação e criptografia (para dados em trânsito e repouso);

5.8.29.2. A autenticação deverá controlar quais aplicações serão autorizadas a obter as senhas armazenadas no cofre de senhas, permitindo validar ao menos a lista de máquinas permitidas (com base em IP/DNS/hostname/sub-rede) e usuários do sistema operacional sob os quais o aplicativo é executado;

5.8.29.3. As credenciais devem ser rotacionadas automaticamente com base nas políticas definidas pelo administrador, sem causar inatividade ou afetar o desempenho do aplicativo;

5.8.29.4. Deve fornecer registros de auditoria (logs), permitindo a auditoria das atividades de solicitação das credenciais pelas aplicações;

5.8.30. Deverá ter a capacidade de gerenciar as credenciais através de um agente (compatível com sistemas Windows e Linux) instalado diretamente em cada servidor de aplicação da CMB (em conformidade com o quantitativo solicitado) ou sem agente (agentless), fazendo o uso de um “Servidor de Credenciais” remoto;

5.8.30.1. O “Servidor de Credenciais” terá o objetivo de fornecer credenciais para aplicativos da CMB via API, possibilitando sua implementação em uma mesma localidade ou localidades distribuídas;

5.8.30.2. O “Servidor de Credenciais” deve ser instalado dentro do ambiente de virtualização da CMB (compatível obrigatoriamente com Hypervisor VMWare), atendendo as seguintes condições:

I. O serviço necessário ao seu funcionamento deverá ser compatível para instalação em sistema operacional Linux ou

Windows, a ser fornecido e instalado pela própria CMB, cabendo à CONTRATADA prestar as devidas orientações para a sua correta configuração e funcionamento;

II. No caso do sistema operacional Windows, o servidor fornecido pela CMB será disponibilizado apenas com as licenças Windows Server Datacenter e CAL (Client Access License), cabendo à CONTRATADA o fornecimento de todas as demais licenças necessárias para o correto funcionamento do serviço;

III. Deverá ser instalado atrás do firewall da CMB, em rede de sua conveniência, de acordo com as recomendações do fabricante;

IV. A CMB ficará responsável pelo seu backup e recuperação em caso de eventual incidente que leve a sua indisponibilidade, cabendo ainda à CONTRATADA prestar todo o apoio necessário para viabilizar esse processo.

5.8.30.3. O “Servidor de Credenciais” deverá ser implementado em arquitetura de alta disponibilidade (High Availability – HA), respeitado o mínimo de 2 (dois) nós redundantes, possibilitando que o serviço continue funcionando mesmo em caso de indisponibilidade ou manutenção do servidor

5.8.30.4. O agente deve fazer uso de cache local seguro, que possua mecanismo de segurança antiadulteração, permitindo um melhor desempenho na recuperação das credenciais, bem como resiliência a interrupções da rede;

5.8.30.5. Devem ser disponibilizados Softwares Development Kit (SDK’s) próprios do fabricante que facilite a integração das aplicações com o gerenciador de credenciais;

5.8.30.6. Deve suportar integração com, no mínimo, as seguintes plataformas para fornecimento de credenciais: JBoss/Wildfly e Tomcat;

5.8.31. Deverá proteger as credenciais administrativas armazenadas localmente nos servidores Linux (físicos ou virtuais);

5.8.31.1. As funcionalidades devem ser providas por meio de agente instalado localmente no sistema operacional, devendo apresentar ao menos a seguinte compatibilidade: Red Hat Enterprise, SUSE Linux Enterprise e Ubuntu;

5.8.31.2. Deve garantir o controle e bloqueio de comandos, mesmo quando o acesso for realizado diretamente no servidor de destino (sem a intermediação da solução), assegurando que as políticas de segurança sejam aplicadas independentemente do método de acesso;

5.8.31.3. Deve disponibilizar, como conjunto mínimo de atividades controladas, as seguintes operações: criação, exclusão e mudança de nome de arquivos/diretórios, mudança do dono ou permissão de arquivos/diretórios e criação de ligações entre arquivos;

5.8.31.4. Deve permitir a implementação de restrições de maneira global ou em uma conta de usuário/grupo de maneira granular;

5.8.31.5. Realizar o controle mediante interceptação dos comandos antes da sua execução, possibilitando a liberação de comandos privilegiados para usuários comuns de forma segura, provendo um controle completo de comandos. Para uma definição ampla dos comandos a serem controlados, a solução deve permitir ao menos a criação uma lista de comandos permitidos e bloqueados (whitelisting/blacklisting), bem como a utilização de coringas (wildcard);

5.8.31.6. Deve permitir que todos os comandos executados nos sistemas monitorados sejam registrados em formato de texto no repositório seguro de credenciais para fins de auditoria;

5.8.31.7. Deve permitir a atribuição de permissões a usuários/grupos, incluindo aqueles integrados ao Active Directory, oferecendo a capacidade de verificar a identidade da pessoa que executa comandos localmente no dispositivo alvo através de autenticação via usuário da ferramenta, LDAP ou RADIUS;

5.8.31.8. Deve possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independente da definição realizada pelo usuário ou seu perfil. Sendo exigido, no mínimo, as seguintes variáveis: PATH, ENV, BASH_ENV, GLOBIGNORE e SHELLOPTS;

5.8.31.9. Deve permitir mapear e coletar atividades regulares de usuários através do modo observação, agregando e exportando os resultados para um perfil;

5.8.31.10. Deve implementar mecanismos que possibilitem aos usuários a execução de comandos específicos e a condução de sessões remotas, fundamentados em regras predefinidas, sem a necessidade de autenticação direta com credenciais privilegiadas.

5.8.32. Deverá proteger as credenciais administrativas armazenadas localmente nos desktops e servidores Windows (físicos ou virtuais);

5.8.32.1. As funcionalidades devem ser providas por meio de agente instalados localmente no sistema operacional, devendo apresentar ao menos a seguinte compatibilidade: Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10 e Windows 11;

5.8.32.2. Deve implementar regras para controle de comandos e aplicações permitidas/bloqueadas, além do nível de privilégio necessário para sua execução, fazendo uso das funcionalidades presentes no próprio sistema operacional, independente se o acesso for realizado diretamente ao servidor ou por intermédio da solução;

5.8.32.3. Deve oferecer opção de execução sem aviso (sem que o usuário precise ser notificado ou solicitar essa elevação) de aplicações que exijam acesso privilegiado;

5.8.32.4. Deve exibir a reputação dos arquivos executados advinda de ao menos 1 (uma) fonte externa, além de disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;

5.8.32.5. Deve implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;

5.8.32.6. Deve permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;

5.8.32.7. Deve permitir a criação de políticas reutilizáveis, contendo ao menos os seguintes tipos de aplicações ou arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX e objetos COM;

5.8.32.8. Deve implementar a verificação de checksum do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;

5.8.32.9. Deve implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;

5.8.32.10. Deve utilizar eventos reportados na interface da ferramenta para criação de novas políticas ou incluí-los em políticas existentes;

5.8.32.11. Deve permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;

5.8.32.12. Deve impedir a desativação das funcionalidades instaladas no sistema operacional sem autorização e/ou registro da atividade por meio da interface de gerência;

5.8.32.13. Deve disponibilizar o registro das atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;

5.8.32.14. Deve permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;

5.8.32.15. Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional ou órgãos de controle de ameaças, como por exemplo o VirusTotal.com ou similares.

5.8.32.16. Deve permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;

5.8.32.17. Deve permitir ao usuário final a solicitação de liberação de atividades específicas;

5.8.32.18. Deve permitir a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;

5.8.32.19. Deve implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;

5.8.32.20. Deve oferecer mecanismos para monitoramento de atividade maliciosa dos processos em execução, visando detectar tentativas de roubo de credenciais;

5.8.32.21. Deve alertar, reportar e bloquear atividade anômala de arquivos e usuários durante a interação com bases de senhas no formato hash, como por exemplo, SAM local e LSASS;

5.8.32.22. Deve permitir o envio de arquivos suspeitos para soluções de análise de ameaça do tipo Sandbox;

5.8.32.23. Deve permitir a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;

5.8.32.24. Deve permitir criar uma whitelist, onde é configurado todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada;

5.8.32.25. Deve possuir uma integração com Windows UAC (User Account Control), e conter relatórios do uso de prompts aos usuários feitos pelo UAC;

5.8.32.26. Deve suportar a guarda de políticas de hosts que não façam parte do Active Directory;

5.8.32.27. Deve manter todas as políticas e serem aplicadas ao ativo em cache, ainda que este não esteja conectado à rede corporativa;

5.8.32.28. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada;

5.8.33. Deverá disponibilizar um cofre de senhas para uso dos funcionários da CMB, fornecendo um método amigável para armazenamento e gerenciamento das credenciais corporativas, além de possibilitar o seu compartilhamento seguro com os demais colaboradores;

5.8.33.1. Além de credenciais básicas (usuário e senha), o cofre deverá ter a capacidade de armazenar outros tipos de informações, tais como: chaves de licença, números de série, PINs e quaisquer outros tipos de segredos confidenciais;

5.8.33.2. Deve contar com uma extensão de navegador compatíveis minimamente com Google Chrome, Mozilla Firefox e Microsoft Edge;

5.8.33.3. A extensão do navegador deverá reconhecer automaticamente quando novas senhas forem inseridas pelos usuários nas aplicações e oferecer a possibilidade de salvá-las no cofre, deverá auxiliar os usuários na geração de senhas complexas e possuir recurso para autopreenchimento das credenciais armazenadas;

5.8.33.4. Deve permitir, a partir da própria extensão do navegador, que o usuário possa efetuar a autenticação necessária para acesso às credenciais salvas, de acordo com a política definida;

5.8.33.5. Deve permitir que o administrador possa determinar quais usuários podem visualizar, editar ou compartilhar credenciais.

5.8.34. Deverá possuir "alertas" pré-definidos nativamente na solução, possibilitando inclusive o seu envio automático por email;

5.8.35. Deverá permitir a criação e customização de dashboards e relatórios;

5.8.36. Todo o conjunto de funcionalidades disponibilizadas para solução tecnológica ofertada deverá trabalhar de forma integrada, oferecendo uma visibilidade unificada das informações.

APENSO B – ACORDO DE CONFIDENCIALIDADE

O presente acordo é celebrado entre **CASA DA MOEDA DO BRASIL**, empresa pública federal criada pela Lei nº 5.895, de l9.06.73, com sede em Brasília - DF, estabelecimento fabril na Rua René Bittencourt, nº 371, Distrito Industrial de Santa Cruz e escritório na Praia do Flamengo, n.º 66, bloco B/19º andar, Município do Rio de Janeiro, inscrita no Cadastro Nacional da Pessoa Jurídica sob nº 034.164.319/0005-06, doravante denominada **CMB**, neste ato representada pelo gestor do Contrato _____, na forma do seu Estatuto Social, aprovado em Assembleia Geral Extraordinária realizada em 31 de julho de 2018 e publicado no D.O.U do dia 12/09/2018 e a empresa _____, com sede em _____, inscrita no Cadastro Nacional da Pessoa Jurídica sob nº _____, doravante denominada **CONTRATADA**, neste ato representada por seu preposto_____.

CONSIDERANDO:

- Que a CMB é uma empresa pública federal provedora de soluções de segurança nos segmentos de meio circulante e pagamento, identificação, rastreabilidade, autenticidade, controle fiscal e postal;
- O CONTRATO de N.º _____ / 20_____ firmado entre as PARTES, doravante denominado CONTRATO PRINCIPAL, onde a CONTRATADA poderá ter acesso às informações sigilosas da CMB;
- A necessidade de ajustar as condições de acesso a essas informações sigilosas, definir as regras para o seu uso e proteção, bem como as penalidades cabíveis em caso de descumprimento;
- Que para alcançar tais finalidades as PARTES se comprometem a proteger as informações compartilhadas de acordo com a forma e as condições a seguir estabelecidas.

Resolvem as PARTES acima qualificadas firmar o presente ACORDO DE CONFIDENCIALIDADE, vinculado ao CONTRATO PRINCIPAL, para a manutenção do sigilo e do caráter de confidencialidade das informações transmitidas entre as PARTES no desenvolvimento das tratativas preliminares e na execução do objeto descrito na cláusula primeira, observado o prazo previsto para as obrigações firmadas neste instrumento de ajuste.

CLÁUSULA PRIMEIRA – OBJETO DO ACORDO

O objeto deste ACORDO DE CONFIDENCIALIDADE é estabelecer as condições de sigilo, confidencialidade e uso limitado das informações transmitidas pelas PARTES.

CLÁUSULA SEGUNDA - DEFINIÇÕES

2.1 – Parte Divulgadora: parte transmissora das informações confidenciais.

2.2 – Parte Receptora: parte receptora das informações confidenciais.

2.3 – Informação Confidencial: toda informação revelada a respeito ou associada ao objeto do CONTRATO PRINCIPAL, transmitida sob a forma escrita, verbal, eletrônica ou por quaisquer outros meios, incluindo mas não se limitando à informação relativa às operações, processos, planos ou intenções, reuniões, conversações, negociações, informações sobre produção, instalações, equipamentos, estratégias empresariais, oportunidades de negócio, segredos de negócio, segredos de fábrica, dados comerciais, dados contábeis, balanços, habilidades especializadas, know-how, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, química, produtos, amostras, insumos, diagramas, desenhos de esquema industrial, descobertas, ideias, conceitos, patentes ou pedidos de patentes, programas de computadores, códigos-fonte, propriedade intelectual, matrizes de custos, composição de preços, planos de ação, características de produtos, relação de clientes, independentemente do suporte físico da informação revelada, salvo se constituírem uma das exceções estabelecidas na CLÁUSULA TERCEIRA.

CLÁUSULA TERCEIRA – OBRIGAÇÃO DE CONFIDENCIALIDADE

3.1 – As PARTES reconhecem que as referências do item 2.3 da Cláusula Segunda deste ACORDO DE CONFIDENCIALIDADE são meramente exemplificativas, e que outras hipóteses de confidencialidade que venham a ser como tal definidas pelas PARTES no futuro deverão ser mantidas sob sigilo.

3.2 –Em caso de dúvida acerca da natureza confidencial de determinada informação, a PARTE RECEPTORA deverá mantê-la sob sigilo até que venha a ser autorizado expressamente pelo Representante Legal da PARTE DIVULGADORA a tratá-la de forma distinta. Em hipótese alguma a ausência de manifestação expressa da PARTE DIVULGADORA poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA QUARTA – ABRANGÊNCIA

As obrigações de confidencialidade assumidas pelas PARTES no presente ACORDO DE CONFIDENCIALIDADE não se aplicam, entretanto, às informações:

4.1 – Que a PARTE RECEPTORA possa comprovar que já eram de domínio público ou que se tornaram disponíveis para o público por outro meio sem sua interferência;

4.2 – Que já se encontrem de forma legítima sob a posse da PARTE RECEPTORA anteriormente à prestação das informações pela PARTE DIVULGADORA, conforme se comprovar por registros escritos e documentos formais;

4.3 – Que tenham sido recebidas pela PARTE RECEPTORA de terceiros que não possuíam, quando da transferência de informações, obrigações de confidencialidade perante a PARTE DIVULGADORA;

4.4 – Que tenham sido desenvolvidas de forma independente pela PARTE RECEPTORA, conforme se comprovar por registros escritos e documentos formais;

4.5 – Que sejam objeto de autorização de divulgação expressa e por escrito pelo Representante Legal da PARTE DIVULGADORA.

4.6 – Cuja revelação às entidades e órgãos do Estado competentes seja exigida por lei, comprometendo-se as PARTES com a obrigação de pronta notificação da requisição das informações ao Representante Legal da PARTE DIVULGADORA, limitando-se tal revelação ao mínimo necessário ao atendimento das determinações e diretrizes legais.

CLÁUSULA QUINTA – FINALIDADES DO USO DAS INFORMAÇÕES

As informações prestadas pela PARTE DIVULGADORA deverão ser usadas pela PARTE RECEPTORA exclusivamente para o estabelecimento de tratativas e execução de negócios com a PARTE DIVULGADORA.

CLÁUSULA SEXTA – EXTENSÃO A COLABORADORES

As informações prestadas pela PARTE DIVULGADORA não serão de modo algum distribuídas, reveladas ou divulgadas a terceiros pela PARTE RECEPTORA, exceto para seus empregados, funcionários, prepostos, prestadores de serviços, subcontratados e demais colaboradores, desde que tenham necessidade justificada de ter conhecimento das referidas informações confidenciais e que, previamente, estejam obrigados à confidencialidade por compromisso formal.

CLÁUSULA SÉTIMA – CONFIDENCIALIDADE DAS AMOSTRAS

7.1 – A PARTE RECEPTORA obriga-se a tratar quaisquer amostras recebidas da PARTE DIVULGADORA como informações confidenciais, sem que se envolva ou sequer permita, sem o consentimento expresso, por escrito, da PARTE DIVULGADORA, qualquer análise da composição, desmontagem, descompilação, ou engenharia reversa das amostras.

7.2 – A PARTE RECEPTORA manterá em sigilo quaisquer informações obtidas da inspeção das amostras, bem como os resultados de sua avaliação das amostras.

CLÁUSULA OITAVA – RESPONSABILIDADE

8.1 – O descumprimento de quaisquer das cláusulas do presente ACORDO DE CONFIDENCIALIDADE acarretará a responsabilidade civil, criminal e administrativa da parte responsável, bem como de todos que, comprovadamente, estiverem envolvidos no respectivo descumprimento ou violação. As PARTES responderão por qualquer revelação não autorizada, efetuada por qualquer dos seus empregados ou contratados que tenham recebido quaisquer informações confidenciais e tomará as providências necessárias para impedi-los de revelar ou utilizar, de forma não autorizada, as informações confidenciais.

8.2 – A PARTE RECEPTORA de informações confidenciais protegidas por este ACORDO DE CONFIDENCIALIDADE que violar as obrigações nele previstas sujeita-se ao pagamento de indenização e/ou de ressarcimento à PARTE DIVULGADORA pelas perdas, danos, lucros cessantes, danos indiretos a que der causa e quaisquer outros prejuízos patrimoniais ou morais suportados pela PARTE DIVULGADORA.

8.3 – A PARTE DIVULGADORA assume toda e qualquer responsabilidade pela titularidade de direitos da propriedade intelectual e demais ativos intangíveis cujas informações sejam transmitidas nessa condição à PARTE RECEPTORA, obrigando-se a responder administrativa, civil e penalmente por qualquer reclamação de terceiros quanto à divulgação não autorizada de tais informações à PARTE RECEPTORA.

8.4 – A PARTE RECEPTORA é responsável pela devida guarda das informações confidenciais e pela pronta notificação da PARTE DIVULGADORA, por escrito, sobre qualquer perda ou destruição dessas informações, incluindo originais e cópias, comprometendo-se a empreender esforços para a localização, recuperação e devolução das informações confidenciais perdidas ou destruídas.

8.5 – Considerando a natureza confidencial e a relevância das informações objeto deste Contrato, e em caso de descumprimento de quaisquer das obrigações aqui estabelecidas, especialmente aquelas relacionadas à confidencialidade e ao sigilo das informações, fica estabelecida uma cláusula penal de até 10 % (dez por cento) sobre o valor total do presente Contrato, a ser paga pela PARTE RECEPTORA em

favor da PARTE DIVULGADORA, a título de multa. A presente cláusula penal não impede a PARTE DIVULGADORA de pleitear, judicial ou extrajudicialmente, a reparação de perdas e danos comprovadamente sofridos que excedam o valor da multa ora estipulada, renunciando as PARTES, desde já, a qualquer alegação de que a cobrança da multa implica renúncia ao direito de indenização suplementar.

CLÁUSULA NONA – DEVOLUÇÃO E DESCARTE DE INFORMAÇÕES

A PARTE RECEPTORA recolherá e encaminhará à PARTE DIVULGADORA, após solicitação formal desta, todo e qualquer material que contenha as informações confidenciais objeto do presente ACORDO DE CONFIDENCIALIDADE, inclusive os documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob controle da PARTE RECEPTORA ou sob a posse de seus empregados, prepostos, prestadores de serviço e fornecedores, com vínculo empregatício ou eventual, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial a que haja obtido acesso.

CLÁUSULA DÉCIMA – PROGRAMA DE INTEGRIDADE

10.1 - Na execução do presente ACORDO DE CONFIDENCIALIDADE é vedado à CMB e à CONTRATADA e/ou a empregado seu, e/ou a preposto seu, e/ou a gestor seu: a) prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público ou a quem quer que seja, ou a terceira pessoa a ele relacionada; b) criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o presente Acordo; c) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações do presente Acordo, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; d) manipular ou fraudar o equilíbrio econômico-financeiro do presente Acordo; ou e) de qualquer maneira fraudar o presente Acordo; assim como realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº 12.846/2013 e suas alterações, do Decreto nº 8420/2015 ou de quaisquer outras leis ou regulamentos aplicáveis (“Leis Anticorrupção”), ainda que não relacionadas com o presente Acordo.

10.2 – As PARTES se comprometem com a integridade nas relações público-privadas e com as orientações e políticas da CMB, inclusive com previsão de aplicação do Programa de Integridade, se for o caso, principalmente com relação à vedação de práticas de fraude e corrupção – materializada por declaração de terceiro.

10.3 – Caso CONTRATADA pratique atos lesivos à administração pública, nacional ou estrangeira, estará sujeita a rescisão contratual sem prejuízo de outras sanções legais ou contratuais.

10.4 – Em caso de ato de corrupção a parte envolvida será responsabilizada.

10.5 – As PARTES se comprometem ao estrito cumprimento ao Programa de Integridade da CMB.

CLÁUSULA DÉCIMA PRIMEIRA – RESOLUÇÃO DE DISPUTAS E LITÍGIOS

11.1 – Disputas e litígios concernentes ao presente ACORDO DE CONFIDENCIALIDADE serão dirimidas, preferencialmente, por resolução amigável entre as PARTES.

11.2 – Para os casos em que não alcançada a resolução amigável de disputas e litígios concernentes ao presente ACORDO DE CONFIDENCIALIDADE, reconhecem as PARTES como competente para resolução judicial o foro da Justiça Federal da Seção Judiciária do Rio de Janeiro.

CLÁUSULA DÉCIMA SEGUNDA – DISPOSIÇÕES FINAIS

12.1 – O presente ACORDO DE CONFIDENCIALIDADE somente poderá ser alterado, substituído ou cancelado por outro acordo celebrado por escrito e firmado pelas PARTES.

12.2 – Nenhuma das PARTES poderá ceder seus direitos ou obrigações decorrentes do presente ACORDO DE CONFIDENCIALIDADE sem o consentimento por escrito da outra PARTE.

12.3 – As disposições do presente ACORDO DE CONFIDENCIALIDADE não serão interpretadas de modo a representar a transferência de titularidade de direitos de propriedade intelectual ou demais ativos intangíveis entre as PARTES, assim como não representarão a formação de *joint venture*, sociedade, ou operação societária entre as PARTES pactuantes.

12.4 – O presente ACORDO DE CONFIDENCIALIDADE é válido pelo prazo de até 5 (cinco) anos contados do encerramento do CONTRATO PRINCIPAL.

E por estarem assim justas e contratadas, as PARTES, juntamente com as testemunhas, assinam o presente ACORDO DE CONFIDENCIALIDADE, em duas vias de igual teor e forma.

_____

Cidade, dia, mês e ano

_____	_____
CMB – Gestor do Contrato	PREPOSTO

Testemunhas:

_____	_____
Identidade (RG):	Identidade (RG):

APENSO C - TERMO DE ACEITE DEFINITIVO

IDENTIFICAÇÃO DAS PARTES

Razão Social (Contratante): Casa da Moeda do Brasil – Parque Industrial do Rio de Janeiro/RJ	CNPJ/MF: 34.164.319/0005-06
Razão Social (Contratada):	CNPJ/MF:

IDENTIFICAÇÃO DO INSTRUMENTO CONTRATUAL

Número do Contrato:
Descrição do(s) Objeto(s):

Atestamos que o(s) objeto(s) acima identificado(s) foi(ram) avaliado(s) quanto à conformidade com as especificações definidas no Termo de Referência, não apresentando problemas ou divergências com as exigências estabelecidas.

_____

Cidade, dia, mês e ano

_____ _____

CMB – Fiscal do Contrato CONTRATADA

APENSO D - NÍVEIS MÍNIMOS DE SERVIÇO (NMS)

Nº	INDICADOR	MÉTRICA	REFERÊNCIA	GLOSA	
1	Índice de disponibilidade mensal das soluções gerenciadas	Porcentagem (%) = (Total de tempo com disponibilidade no mês / Total de tempo no mês) * 100	>=99,7%	Se < 99,7%	1%
				Se <= 99,4%	2%
				Se <= 99%	3%
2	Índice de chamados finalizados adequadamente	Porcentagem (%) = (Total de chamados com resolução / Total de chamados finalizados) * 100	>=90%	Se < 90%	0,25%
				Se <= 79%	0,5%
				Se <= 69%	1%
3	Prazo máximo para correção de falhas, indisponibilidade ou degradação da qualidade das soluções	**Atuando de forma remota:** Tempo = Hora do início da indisponibilidade – Hora do restabelecimento **Atuando de forma presencial:** Tempo = Hora do primeiro acesso à solução – Hora do restabelecimento	<= 6 horas	0,5% (+0,25% por cada hora excedente até o máximo de 10 horas)	
4	Prazo máximo para resolução de requisições relacionadas à gestão de políticas de segurança	Tempo = Hora do início da requisição – Hora da conclusão	De 1 a 10 <= 60 minutos Acima de 10 <= 120 minutos	0,5% (+0,25% por cada dez minutos excedentes até o máximo de 100 minutos)	
5	Prazo máximo para resolução de requisições relacionadas à gestão de configurações gerais	Tempo = Hora do início da requisição – Hora da conclusão	De 1 a 10 <= 90 minutos Acima de 10 <= 150 minutos	0,25% (+0,25% por cada dez minutos excedentes até o máximo de 100 minutos)	
6	Prazo máximo para resolução de requisições de upgrade/downgrade de sistema/firmware	Tempo = Hora do início da requisição – Hora da conclusão	<= 24 horas	0,5% (+0,25% por cada hora excedente até o máximo de 10 horas)	
7	Prazo máximo para resolução de requisições de criação/customização de dashboards, relatórios técnicos e alertas	Tempo = Hora do início da requisição – Hora da conclusão	<= 4 horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)	
8	Prazo máximo para resolução de requisições de integração de soluções de terceiros via API	Tempo = Hora do início da requisição – Hora da conclusão	<= 24 horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)	
9	Prazo máximo para resolução de requisições de inclusão de ativos ao Incident Management Platform	Tempo = Hora do início da requisição – Hora da conclusão	<= 6 horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)	
10	Prazo máximo para resolução de requisições de criação/customização de simulações de ataque	Tempo = Hora do início da requisição – Hora da conclusão	<= 8 horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)	
11	Prazo máximo para resolução de requisições de criação/customização de playbooks	Tempo = Hora do início da requisição – Hora da conclusão	<= 6 horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)	

12	Prazo máximo para a iniciar atendimento de requisições de takedown	Tempo = Hora do início da requisição – Hora da conclusão	<= 2 horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
13	Prazo máximo para a resolução de requisições de análise de incidentes suspeitos pontuais	Tempo = Hora do início da requisição – Hora da conclusão	<= 6 horas	0,5% (+0,25% por cada hora excedente até o máximo de 10 horas)
14	Prazo máximo para a resolução de requisições de análise de vulnerabilidades pontuais	Tempo = Hora do início da requisição – Hora da conclusão	<= 4 horas	0,5% (+0,25% por cada hora excedente até o máximo de 10 horas)
15	Prazo máximo para iniciar atendimento de requisições de apoio/auxílio na execução de atividades operacionais nas soluções	Tempo = Hora do início da requisição – Hora da conclusão	<= 1 hora	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
16	Prazo máximo para finalização da “Triagem Básica do Incidente” e envio do “Relatório Preliminar do Incidente” para a CMB	Tempo = Hora do início o evento – Hora do envio do relatório	<= 1 Hora	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
17	Prazo máximo para contenção de incidente (prioridade P1)	Tempo = Hora do início da contenção – Hora do fim da contenção	<= 40 minutos	1% (+0,25% por cada dez minutos excedentes até o máximo de 100 minutos)
18	Prazo máximo para contenção de incidente (prioridade P2)	Tempo = Hora do início da contenção – Hora do fim da contenção	<= 1 Hora	0,5% (+0,25% por cada hora excedente até o máximo de 10 horas)
19	Prazo máximo para contenção de incidente (prioridade P3)	Tempo = Hora do início da contenção – Hora do fim da contenção	<= 2 Horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
20	Prazo máximo para contenção de incidente (prioridade P4)	Tempo = Hora do início da contenção – Hora do fim da contenção	<= 3 Horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
21	Prazo máximo para contenção de incidente (prioridade P5)	Tempo = Hora do início da contenção – Hora do fim da contenção	<= 4 Horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
22	Prazo máximo para envio do “Plano de Erradicação e Recuperação do Incidente”	Tempo = Hora do fim da contenção – Hora da entrega do plano	<= 4 Horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
23	Prazo máximo para envio do “Relatório Completo do Incidente”	Tempo = Hora do fim da investigação completa do incidente – Hora do envio do relatório	<= 3 Hora	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
24	Prazo máximo para envio do “Relatório de Correção das Vulnerabilidades”	Tempo = Hora do fim da verificação das vulnerabilidades – Hora da entrega do relatório	<= 2 Hora	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)

25	Prazo máximo para envio do “Relatório de problemas/falhas” (Ambiente de Homologação)	Tempo = Hora que o impacto foi identificado – Hora do envio do relatório	<= 8 Horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
26	Prazo máximo para envio do “Relatório de problemas/falhas” (Ambiente de Produção)	Tempo = Hora que o impacto foi identificado – Hora do envio do relatório	<= 6 Horas	0,5% (+0,25% por cada hora excedente até o máximo de 10 horas)
27	Prazo máximo para envio do “Relatório de Inviabilidade de Correção”	Tempo = Hora da identificação da inviabilidade de correção – Hora do envio do relatório	<= 8 Horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
28	Prazo máximo para aplicação das correções de vulnerabilidades (Ambiente de Homologação)	Tempo = Hora da aprovação da correção – Hora da conclusão das correções	<= 48 horas	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)
29	Prazo máximo para aplicação das correções de vulnerabilidades (Ambiente de Produção)	Tempo = Hora da aprovação da correção – Hora da conclusão das correções	<= 72 horas	0,5% (+0,25% por cada hora excedente até o máximo de 10 horas)
30	Prazo máximo para envio do “Relatório de Reavaliação de Vulnerabilidades”	Tempo = Hora do fim da aplicação das correções – Hora do envio do relatório	<= 2 Hora	0,25% (+0,25% por cada hora excedente até o máximo de 10 horas)

Nº	INDICADOR	REFERÊNCIA	GLOSA
31	Fraudar, manipular ou descaracterizar indicadores de níveis de serviço	Por ocorrência	2%
32	Deixar de comunicar a CMB sobre quaisquer problemas ou anomalias identificadas no contrato	Por ocorrência	1%
33	Deixar de aplicar controles de segurança adequados para garantir a confidencialidade dos dados da CMB que vier a receber ou ter acesso ao longo da vigência contratual	Por dia de descumprimento	0,5% (+0,25% por dia de descumprimento até o máximo de 10 dias)
34	Deixar de adequar a redação de documentos e relatórios gerados quanto à clareza, objetividade, detalhamento técnico e conformidade com as boas práticas e normas aplicáveis	Por ocorrência	0,25%
35	Deixar de colaborar com a CMB na resolução de problemas diversos relacionados ao contrato	Por ocorrência	0,5%
36	Gerar cobranças indevidas sem o consentimento da CMB	Por ocorrência	1%
37	Deixar de enviar profissionais presencialmente à CMB dentro do prazo máximo estipulado	Por dia de descumprimento	1% (+0,25% por dia de descumprimento até o máximo de 10 dias)
38	Deixar de participar de reuniões quando solicitado pela CMB	Por ocorrência	0,5%

39	Deixar de apresentar documentos, relatórios ou fornecer esclarecimentos acerca de quaisquer atividades vinculadas a contratação	Por ocorrência	0,5%
40	Deixar de cumprir o requisito de garantia, suporte técnico e atualização contínua de firmware oficiais do fabricante	Por dia de descumprimento	1% (+0,25% por dia de descumprimento até o máximo de 10 dias)
41	Deixar de cumprir determinações gerais da equipe de fiscalização do contrato	Por ocorrência	0,5%
42	Deixar de apresentar análise de riscos para mudanças com potencial impacto ao ambiente da CMB	Por ocorrência	0,25%
43	Deixar de cumprir qualquer especificação técnica exigida para as soluções tecnológicas requisitadas	Por dia de descumprimento	0,5% (+0,25% por dia de descumprimento até o máximo de 10 dias)
44	Impedir ou dificultar que a CMB (ou instituição independente por ela autorizada) realize auditorias a fim de averiguar o correto cumprimento do contrato	Por ocorrência	2%
45	Deixar de cumprir o período de retenção mínimo estabelecido para os dados armazenados nas soluções	Por GigaByte (GB) perdido	0,5% (+0,25% por cada 10 GB perdidos)
46	Deixar de cumprir qualquer requisito relacionado a infraestrutura necessária para prestação do serviço	Por dia de descumprimento	0,5% (+0,25% por dia de descumprimento até o máximo de 10 dias)
47	Deixar de cumprir qualquer requisito relacionado a qualificação da equipe técnica	Por dia de descumprimento	1% (+0,25% por dia de descumprimento até o máximo de 10 dias)
48	Deixar de comprovar anualmente que está atendendo aos requisitos de qualificação da equipe	Por ocorrência	0,5%
49	Deixar de informar eventual descumprimento dos requisitos de qualificação da equipe técnica	Por ocorrência	0,25%
50	Deixar de substituir profissional a pedido da CMB dentro do prazo máximo estabelecido	Por dia de descumprimento	0,25% (+0,25% por dia de descumprimento até o máximo de 10 dias)
51	Deixar de apresentar “Plano de Capacitação” no prazo máximo estabelecido	Por dia de descumprimento	0,25% (+0,25% por dia de descumprimento até o máximo de 10 dias)
52	Deixar de cumprir o quantitativo mínimo de horas de treinamento estabelecido no “Plano de Capacitação”	Por ocorrência	0,25%

53	Não fornecer ou deixar de fornecer acesso privilegiado aos profissionais da CMB às soluções gerenciadas	Por dia de descumprimento	1% (+0,25% por dia de descumprimento até o máximo de 10 dias)
54	Deixar de colaborar com a CMB no desenvolvimento de planos de ação para resolução de problemas técnicos ou para melhoria contínua do ambiente	Por ocorrência	0,5%
55	Deixar de substituir a solução tecnológica por outra de fabricante distinto no prazo determinado	Por hora de descumprimento	0,5% (+0,25% por cada hora de descumprimento até o máximo de 10 horas)
56	Realizar mudança nas configurações da solução, sem autorização da CMB, que impacte no seu ambiente	Por ocorrência	1%
57	Causar danos diretos ou indiretos aos equipamentos da CMB por negligência ou imperícia	Por ocorrência	2%
58	Deixar de abrir ou acompanhar chamados junto ao fabricante da solução quando necessário	Por ocorrência	0.5%
59	Deixar de monitorar continuamente a disponibilidade e o desempenho das soluções gerenciadas	Por ocorrência	0,25%
60	Deixar de comunicar a CMB sobre qualquer ocorrência de indisponibilidade, problemas de desempenho, mau funcionamento ou anomalias identificadas nas soluções	Por ocorrência	0,5%
61	Deixar de cumprir o prazo máximo de 24 horas de perda de dados para restauração das soluções	Por hora de descumprimento	0,5% (+0,25% por cada hora de descumprimento até o máximo de 10 horas)
62	Deixar de substituir os equipamentos ou componentes físicos instalados nas premissas da CMB no prazo máximo de 72 horas	Por hora de descumprimento	1% (+0,25% por cada hora de descumprimento até o máximo de 10 horas)
63	Deixar de disponibilizar ou inviabilizar o acesso a qualquer canal de atendimento exigido para o suporte técnico	Por dia de descumprimento	0,5% (+0,25% por dia de descumprimento até o máximo de 10 dias)
64	Deixar de realizar o registro das informações nos chamados ou fazê-lo de forma incorreta/incompleta	Por ocorrência	0,25%
65	Deixar de atender qualquer requisito exigido para os canais de atendimento do suporte	Por dia de descumprimento	0,25% (+0,25% por dia de descumprimento até o máximo de 10 dias)
66	Deixar de fazer ou atrasar sem justificativa o escalonamento dos chamados	Por ocorrência	0,25%

67	Deixar de comunicar a CMB sobre mudanças de profissionais constantes da lista de “escalação extraordinária”	Por ocorrência	0,25%
68	Permitir a abertura de chamados por pessoas não autorizadas	Por ocorrência	1%
69	Deixar de comunicar a CMB sobre tentativas de abertura de chamados por pessoas não autorizadas	Por ocorrência	0,25%
70	Realizar mudança de status do chamado indevidamente	Por ocorrência	0,5%
71	Deixar de acompanhar chamados classificados com status de “pendente” dentro dos prazos previstos	Por ocorrência	0,25%
72	Deixar de apresentar “Resoluções Paliativas” para redução ou eliminação de impactos causados no ambiente	Por dia de descumprimento	1% (+0,25% por dia de descumprimento até o máximo de 10 dias)
73	Deixar de apresentar “Resolução Definitiva” (quando disponibilizada) para problema no qual tenha sido adotada uma “Resoluções Paliativas” temporária	Por ocorrência	0,25%
74	Deixar de contabilizar corretamente o tempo de atendimento dos chamados	Por ocorrência	0,5%
75	Deixar de realizar a avaliação semestral do ambiente da CMB (Assessment de Segurança)	Por ocorrência	0,5%
76	Deixar de participar de reuniões dentro do prazo estabelecido em contrato	Por dia de descumprimento	0,25% (+0,25% por dia de descumprimento até o máximo de 10 dias)
77	Deixar de apresentar relatórios no prazo máximo estabelecido ou entregá-los de forma incorreta/incompleta	Por dia de descumprimento	0,25% (+0,25% por dia de descumprimento até o máximo de 10 dias)
78	Deixar de documentar ou implementar mudanças aprovadas pela CMB visando a evolução e amadurecimento dos processos	Por ocorrência	0,25%
79	Deixar de identificar incidentes cibernéticos legítimos	Por ocorrência	1%
80	Realizar a “Triagem Básica do Incidente” de forma incorreta/incompleta	Por ocorrência	0,25%

81	Deixar de comunicar a CMB sobre incidentes cibernéticos identificados no ambiente	Por ocorrência	0,5%
82	Deixar de registrar ou investigar incidentes ou fazê-lo de forma incorreta/incompleta	Por ocorrência	0,5%
83	Deixar de criar ou atualizar “playbooks” para resposta automatizada de incidentes	Por ocorrência	0,25%
84	Deixar de auxiliar a CMB no processo de erradicação do incidente e recuperação dos serviços afetados ou fazê-lo de forma incorreta/incompleta	Por ocorrência	0,5%
85	Deixar de realizar a identificação/descoberta dos ativos nos moldes especificados	Por ocorrência	0,25%
86	Deixar de realizar análise das vulnerabilidades (eliminação de falsos positivos)	Por ocorrência	0,25%
87	Deixar de realizar a verificação de vulnerabilidades no período estabelecido ou fazê-lo de forma incorreta/incompleta	Por ocorrência	0,5%
88	Deixar de classificar e ordenar as vulnerabilidades nos moldes especificados	Por ocorrência	0,5%
89	Aplicar correções de vulnerabilidades sem a aprovação da CMB (Ambiente de Homologação)	Por ocorrência	0,25%
90	Aplicar correções de vulnerabilidades sem a aprovação da CMB (Ambiente de Produção)	Por ocorrência	1%
91	Deixar de auxiliar a CMB no processo de identificação dos problemas/falhas ocasionados pelas correções aplicadas (Ambiente de Homologação)	Por ocorrência	0,25%
92	Deixar de auxiliar a CMB no processo de identificação dos problemas/falhas ocasionados pelas correções aplicadas (Ambiente de Produção)	Por ocorrência	1%
93	Deixar de auxiliar a CMB no processo de retorno (rollback) dos ativos ao seu estado de normalidade (Ambiente de Homologação)	Por ocorrência	0,5%
94	Deixar de auxiliar a CMB no processo de retorno (rollback) dos ativos ao seu estado de normalidade (Ambiente de Produção)	Por ocorrência	2%

95	Deixar de documentar as decisões de “aceitação ao risco” ou fazê-lo de forma incorreta/incompleta	Por ocorrência	0,25%
96	Deixar de cobrar, após o prazo de expiração, a resolução de riscos aceitos pela CMB	Por ocorrência	0,25%
97	Deixar de cumprir qualquer outra obrigação estabelecida no edital e não prevista nesta tabela	Por ocorrência	0,25%

APENSO E - DECLARAÇÃO DE VISTORIA

A empresa _____,
portadora do CNPJ _____, localizada no endereço _____ e representada por _____
declara, para fins de participação no processo licitatório, que vistoriou o ambiente da CMB e tem total conhecimento do objeto licitado no Pregão Eletrônico nº_____/20____, inclusive quanto às suas características, quantitativos e especificidades, reconhecendo que não poderá fazer qualquer tipo de reclamação posterior com relação ao desconhecimento dos detalhes técnicos e operacionais eventualmente não detectados na vistoria.

_____

Cidade, dia, mês e ano

_____

Empregado da CMB

_____

Representante da empresa

APENSO F - PROPOSTA DE PREÇOS

PREGÃO ELETRÔNICO nº_____

RAZÃO SOCIAL:

CNPJ:

ENDEREÇO:

TELEFONE:

E-MAIL:

PLANILHA DE PREÇOS		
Item	**Descrição/Especificação**	**Total Mensal [3]**
1	Serviço Gerenciado de Segurança (Managed Security Services - MSS) com Fornecimento de Soluções Tecnológicas de Cibersegurança [1] [2]	
TOTAL GLOBAL [4] (36 MESES)		

1- **Embora o fornecimento do objeto ocorra por meio de item único, a CONTRATADA deverá obrigatoriamente apresentar proposta com discriminação detalhada de todos os elementos que a compõem, seguindo o modelo de tabela constante deste apenso.**
2- **Na hipótese de serem ofertadas soluções tecnológicas complementares à solução principal, nos termos deste Termo de Referência, estas deverão ser apresentadas como componentes integrantes da solução principal, observando o modelo de tabela indicado.**
3- **O valor apresentado no campo "Total Mensal" deverá corresponder ao somatório de todos os subtotais indicados no modelo de tabela apresentado a seguir.**
4- **O valor apresentado no campo "Total Global" deverá corresponder à multiplicação do valor indicado em "Total Mensal" pelo período de 36 (trinta e seis) meses de vigência contratual.**

DISCRIMINAÇÃO DOS VALORES						
Nome do Componente	**Fabricante**	**Part Number**	**Forma de Fornecimento**	**Qtde. (A)**	**Valor Unitário (B)**	**Valor Mensal (AxB)**
Incident Management Platform						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Network Packet Broker (NPB)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Cyber Threat Intelligence Platform (CTI)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Vulnerability Management Platform						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Breach and Attack Simulation (BAS)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						

Subtotal Mensal						
Secure Access Service Edge (SSE)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Web Application Security Platform						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Unified Identity Security Platform						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Gerenciamento Soluções internas (PENSO H)						
Serviço						
Subtotal Mensal						

APENSO G – COMPROVAÇÃO DE REQUISITOS

REQUISITOS GERAIS			
Item	**Requisito**	**Documento**	**Observação**
1.29.	Todas as soluções tecnológicas ofertadas, em regra, deverão pertencer à fabricantes amplamente consolidados no mercado, não sendo aceitas soluções desenvolvidas pela própria CONTRATADA ou baseadas em softwares projetados para uso genérico, sem a devida customização ou parametrização para atender aos requisitos específicos deste Termo de Referência; 1.29.1. Como referência de fabricantes amplamente consolidados no mercado, serão considerados estudos ou documentos de institutos de análise independente e imparcial: Gartner, Forrester, IDC e ISG Group.		
1.31.	As soluções providas no modelo de Software-as-a-Service (SaaS) deverão oferecer suporte a ambientes multi-tenant, garantindo o isolamento seguro para assegurar que os dados da CMB não sejam acessados pelos demais clientes da CONTRATADA ou fabricante;		
1.33.	A data prevista pelo fabricante para descontinuidade ("end-of-life" ou similar) dos “appliances físicos” ofertados não poderá, no momento da apresentação da proposta, coincidir com o período de vigência contratual;		
1.37.	As soluções ofertadas deverão contar com garantia, suporte técnico e atualização constante oficiais do fabricante, compatíveis com os com níveis de serviço exigidos nesta contratação, durante toda a vigência contratual;		
1.49.	O serviço deverá ser provido, no mínimo, por meio 2 (dois) Centros de Operações de Segurança (Security Operation Center - SOC) físicos redundantes, que devem estar em pleno funcionamento na data da assinatura do contrato, de modo que a indisponibilidade de um deles não afete a continuidade do serviço prestado; 1.49.1. Os SOC’s deverão estar situados no Brasil, guardando uma distância mínima de 50 km (cinquenta quilômetros) entre si, onde ao menos um deles deve estar localizado na região sudeste do país; 1.49.2. Devem possuir UPS (Uninterruptible Power Supply) que permita a continuidade da prestação do serviço na eventualidade de interrupção de curto prazo no fornecimento de energia comercial; 1.49.3. Devem possuir gerador, com acionamento automático, para situações de eventual interrupção prolongada da energia comercial, com autonomia mínima de 72 (setenta e duas) horas.		
1.50.	A CONTRATADA poderá manter parte de sua equipe (Níveis 2 e 3) trabalhando de forma remota. No entanto, é imprescindível garantir a presença constante de profissionais (Nível 1) fisicamente no SOC, assegurando assim o monitoramento, identificação e o tratamento ininterrupto e eficiente de todas as ameaças e incidentes de cibersegurança;		

1.51.	Os SOC's deverão possuir uma estrutura mínima para garantir que os profissionais possam executar suas atividades com o máximo de eficácia e resiliência, tais como: I. Sistema de refrigeração por ar-condicionado; II. Mesas e cadeiras apropriadas; III. Recursos e equipamentos tecnológicos adequados; IV. Estrutura de vídeo centralizada para monitoramento de incidentes em tempo real (Ex. Video Wall, televisores, entre outros).		
1.52.	As soluções tecnológicas deverão ser hospedadas em infraestrutura de Data Center redundantes, o que poderá ocorrer, inclusive de forma híbrida, através das seguintes alternativas: (1) Data Center próprio da CONTRATADA, (2) Data Center de terceiros alocado pela CONTRATADA, (3) Data Center de provedores de cloud públicas de mercado ou (4) Data Center do próprio fabricante da solução tecnológica ofertada; 1.52.1. As soluções deverão ser implementadas de modo que a indisponibilidade de um dos Data Centers não impacte na continuidade do serviço prestado, devendo ter a capacidade de recuperar-se automaticamente de eventuais desastres, garantindo a integridade e continuidade dos acessos aos dados históricos armazenados (respeitado o período máximo de retenção especificado neste documento) e a ingestão de novos dados;		
1.53.	O SOC's e os Data Centers utilizados pela CONTRATADA (principal e redundante) deverão possuir controles de segurança física, de forma a assegurar a proteção das instalações, a prevenção de acessos não autorizados e a rastreabilidade dos acessos realizados aos ambientes que suportem a operação da CMB; 1.53.2. Os SOC's e os Data Centers deverão contar com sistema de CFTV (Circuito Fechado de Televisão) em operação contínua, abrangendo os acessos e áreas críticas, de forma a viabilizar a rastreabilidade das pessoas no ambiente; 1.53.3. Os SOC's e os Data Centers deverão possuir sistema de controle de acesso físico capaz de registrar, de forma individualizada, as entradas e saídas de pessoas, mediante mecanismos de autenticação baseados em biometria, reconhecimento facial ou tecnologia equivalente que assegure identificação inequívoca do indivíduo; 1.53.4. Os SOC's e os Data Centers deverão contar com serviço de vigilância física especializada e armada, em regime contínuo (24x7x365), destinado à proteção patrimonial e à prevenção de acessos físicos não autorizados. Especificamente em relação aos SOC's, esta exigência poderá ser atendida por meio da estrutura de segurança patrimonial já existente na edificação, condomínio corporativo ou instalação onde os mesmos estiverem localizados, não sendo obrigatória a disponibilização de equipe dedicada.		
1.54.	Os SOCs e Data Centers utilizados pela CONTRATADA (principal e redundante), deverão possuir certificação ISO/IEC 27001 válida no momento da contratação, cujo escopo deverá abranger os serviços objeto deste contrato, bem como as instalações e operações dos Data Centers empregados na sua execução, garantindo a conformidade com as melhores práticas de segurança da informação;		
1.55.	A CONTRATADA deverá possuir e manter um plano de continuidade previamente estabelecido, que comprove sua capacidade de recuperação diante de incidentes que afetem a continuidade dos serviços prestados;		

SOLUÇÕES TECNOLÓGICAS DE CIBERSEGURANÇA				
Item	**Documento**	**Página**	**Trecho**	**Observação**
Incident Management Platform				
5.1.1				
5.1.2				
5.1.N				
Network Packet Broker (NPB)				
5.2.1				
5.2.2				
5.2.N				
Cyber Threat Intelligence Platform (CTI)				
5.3.1				
5.3.2				
5.3.N				
Vulnerability Management Platform				
5.4.1				
5.4.2				
5.4.N				
Breach And Attack Simulation (BAS)				
5.5.1				
5.5.2				
5.5.N				

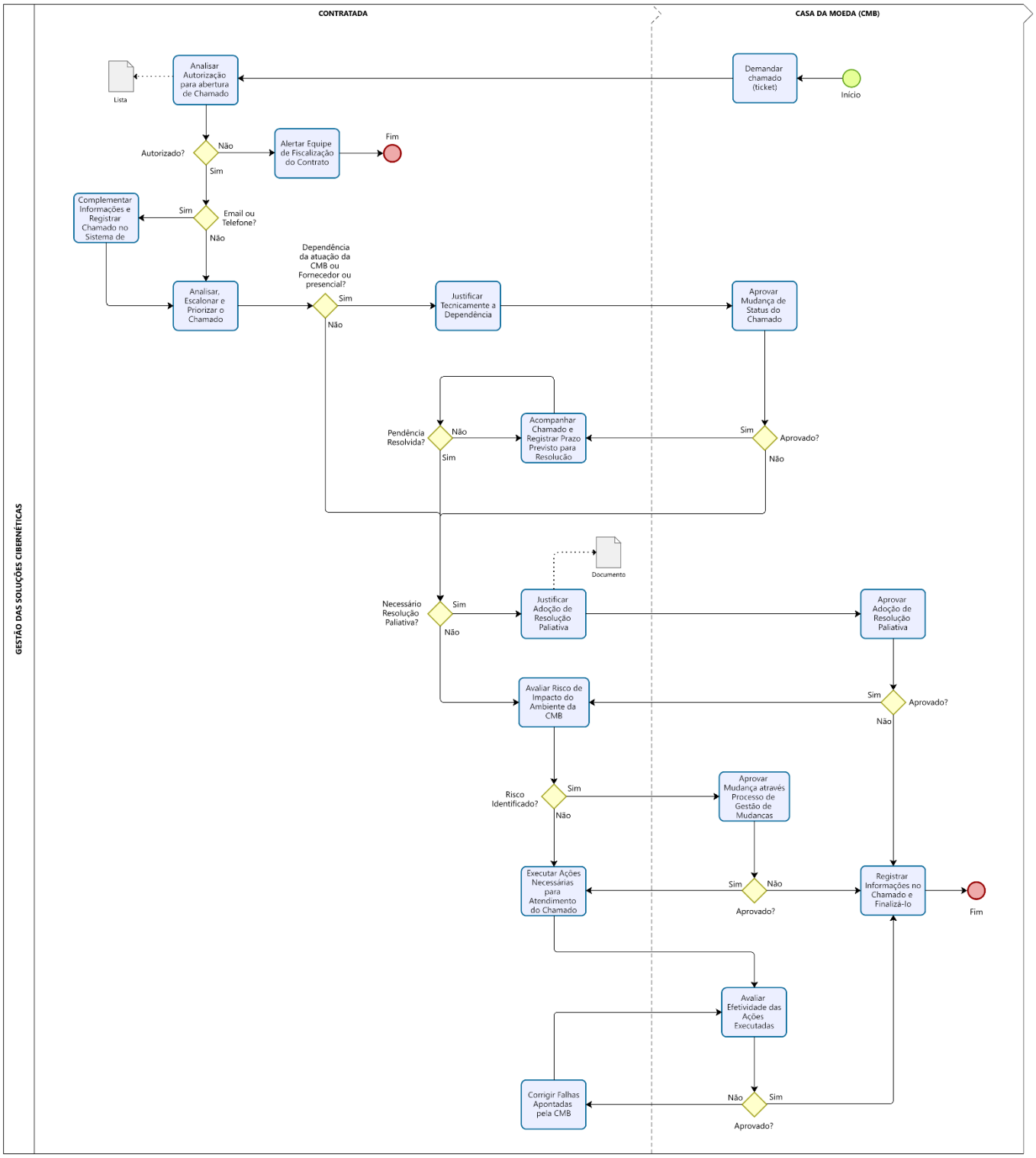
Security Service Edge (SSE)				
5.6.1				
5.6.2				
5.6.N				
Web Application Security Platform				
5.7.1				
5.7.2				
5.7.N				
Unified Identity Security Platform				
5.8.1				
5.8.2				
5.8.N				

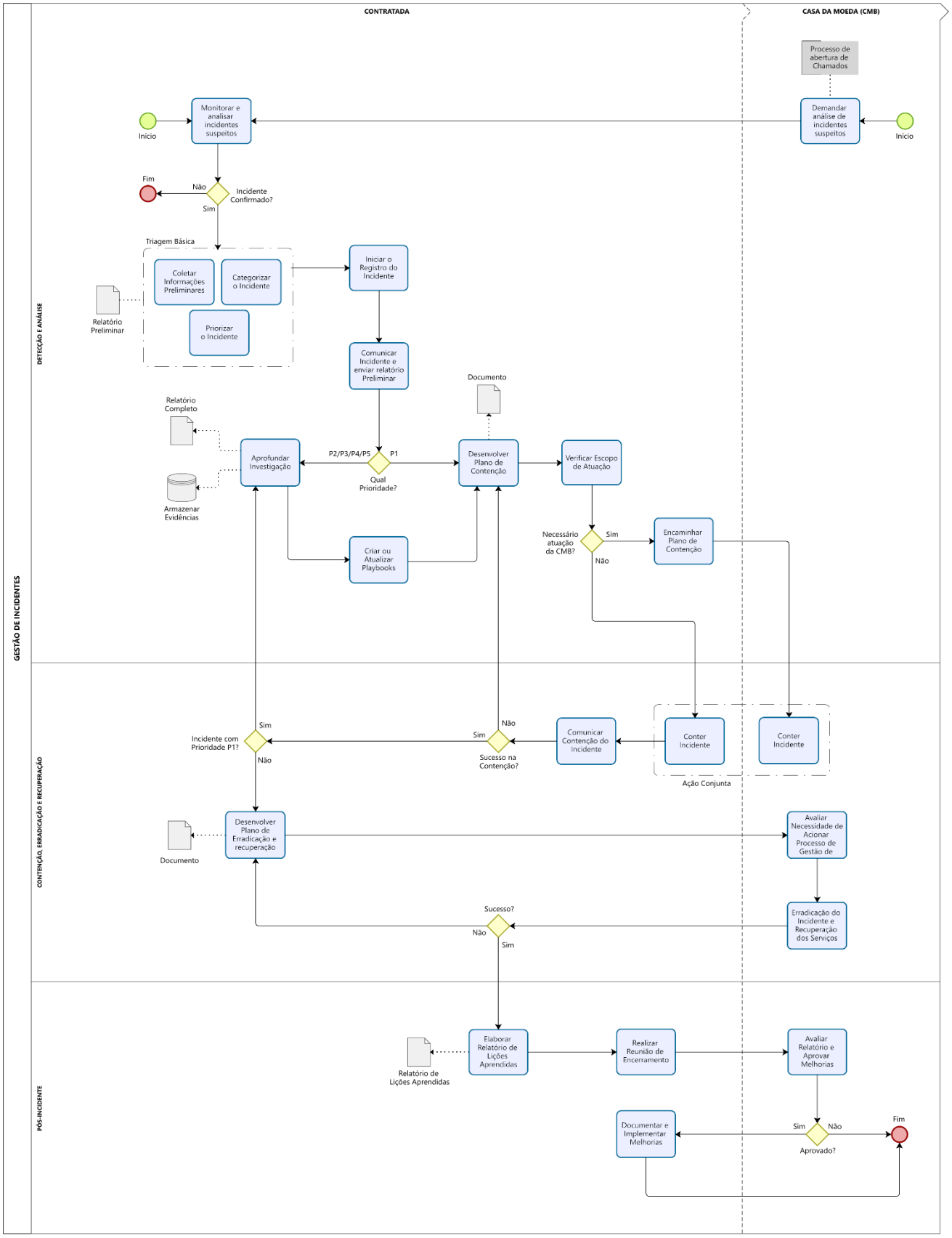
APENSO H - SOLUÇÕES INTERNAS

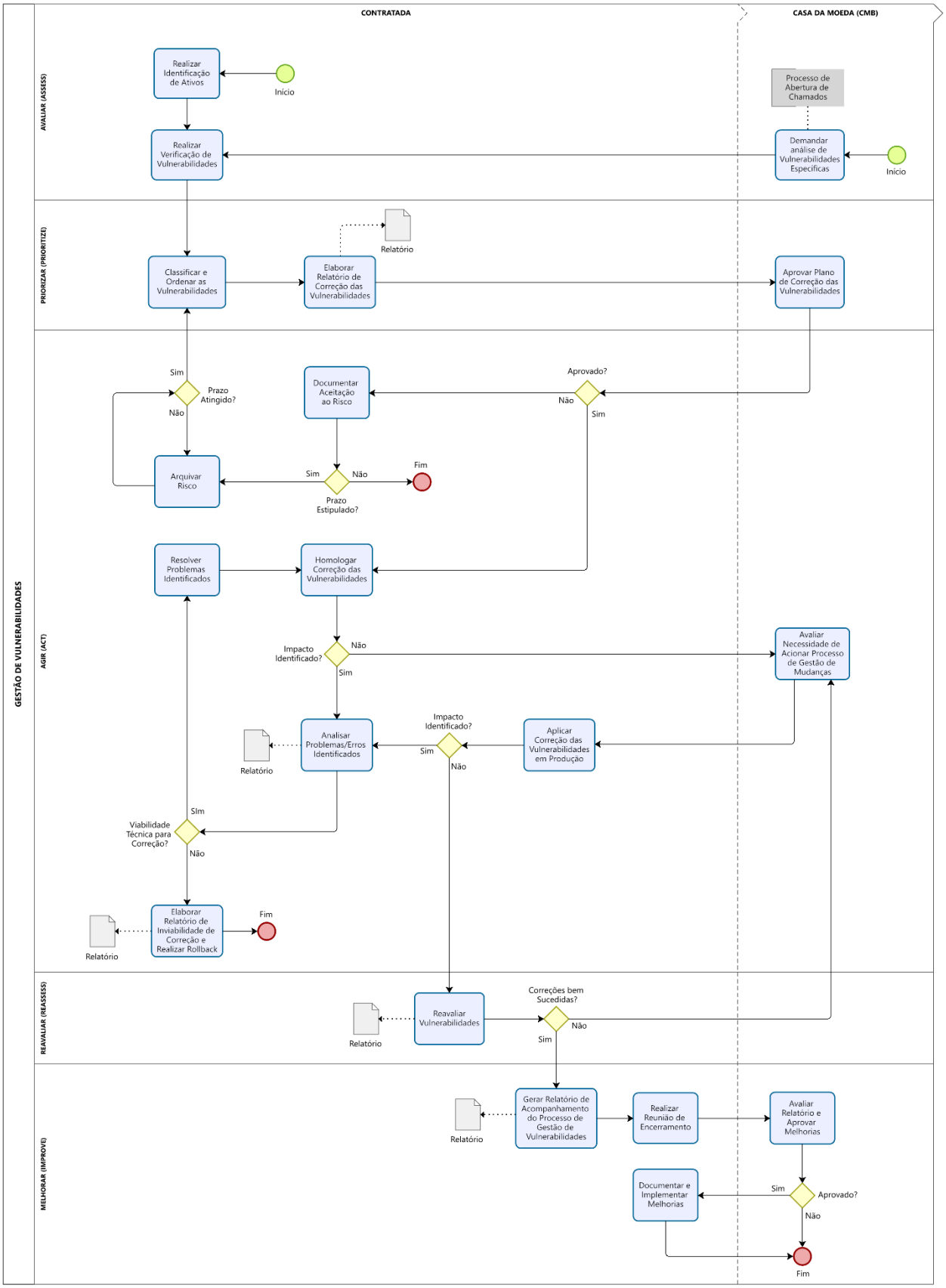
DESCRIÇÃO	FUNCIONALIDADES	LOCAL	QNT
Microsoft Exchange Online Protection (EOP)	Antimalware Anti-spam Anti-phishing Anexos Seguros Links seguros	Cloud	1800 contas
Microsoft Defender for Cloud Apps Discovery	CASB	Cloud	1800 contas
Microsoft Defender for Cloud Apps			
Microsoft Office 365 Cloud App Security			
Trend Micro ApexOne	Anti-malware Web Reputation Firewall Device Control Activity Monitoring Application Control Intrusion Prevention Integrity Monitoring Log Inspection	Cloud	1500 Ativos
Trend Micro Workload Security			410 Ativos
Trend Micro Cloud App Security (CAS)	OFFICE 365: Anti-spam Antimalware File Blocking Web Reputation Sandbox		1800 contas

Fortinet Fortigate Next Generation Firewall (NGFW)	Firewall Antimalware Web Filter DNS Filter Application Control Intrusion Prevention SSL/SSH Inspection	On-premise	3 Clusters (2 nós cada)
Serviço de Anti-DDoS prestados pelas operadoras de telecomunicações	Anti-DDoS	Cloud	2 links de internet

APENSO I – MODELAGEM DOS PROCESSOS

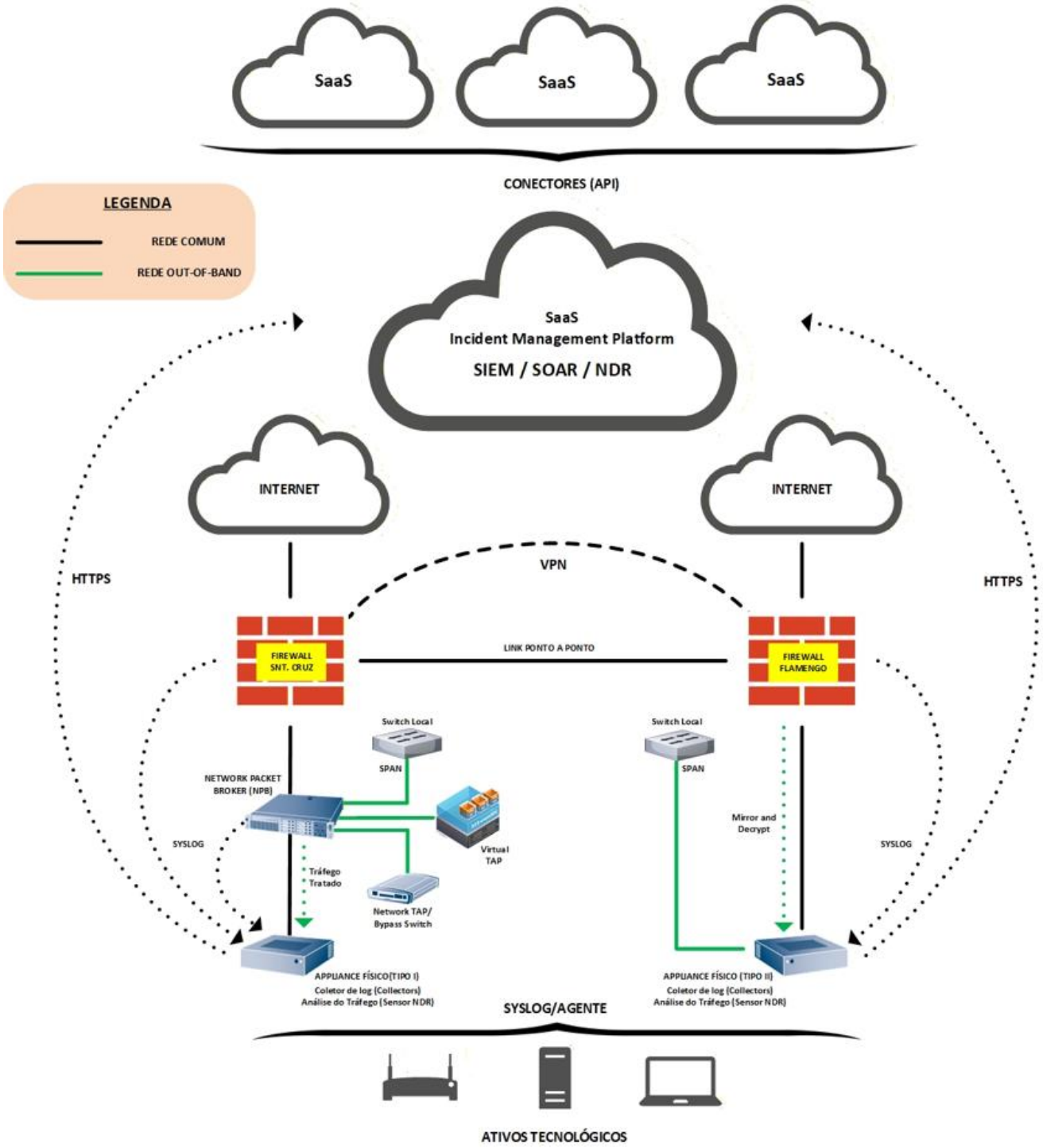


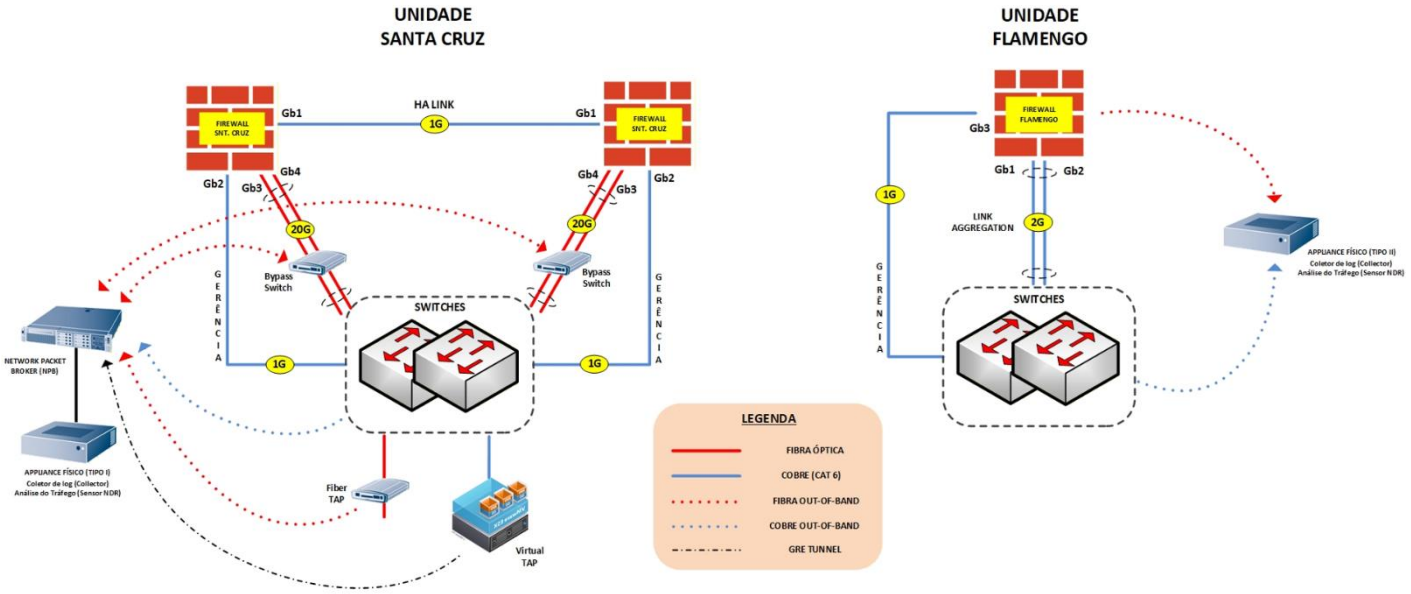

CONTRATADA
CASA DA MOEDA (CMB)
GESTÃO DE INCIDENTES
DETECÇÃO E ANÁLISE
CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO
PÓS-INCIDENTE
Processo de abertura de Chamados
Demandar análise de incidentes suspeitos
Início
Monitorar e analisar incidentes suspeitos
Início
Fim
Não
Incidente Confirmado?
Sim
Triagem Básica
Coletar Informações Preliminares
Categorizar o Incidente
Priorizar o Incidente
Relatório Preliminar
Iniciar o Registro do Incidente
Comunicar Incidente e enviar relatório Preliminar
Documento
Relatório Completo
Aprofundar Investigação
Armazenar Evidências
P2/P3/P4/P5
P1
Qual Prioridade?
Desenvolver Plano de Contenção
Verificar Escopo de Atuação
Criar ou Atualizar Playbooks
Necessário atuação da CMB?
Sim
Não
Encaminhar Plano de Contenção
Incidente com Prioridade P1?
Sim
Não
Sucesso na Contenção?
Não
Sim
Comunicar Contenção do Incidente
Conter Incidente
Conter Incidente
Ação Conjunta
Documento
Desenvolver Plano de Erradicação e recuperação
Avaliar Necessidade de Acionar Processo de Gestão de
Erradicação do Incidente e Recuperação dos Serviços
Sucesso?
Não
Sim
Relatório de Lições Aprendidas
Elaborar Relatório de Lições Aprendidas
Realizar Reunião de Encerramento
Avaliar Relatório e Aprovar Melhorias
Documentar e Implementar Melhorias
Sim
Não
Aprovado?
Fim

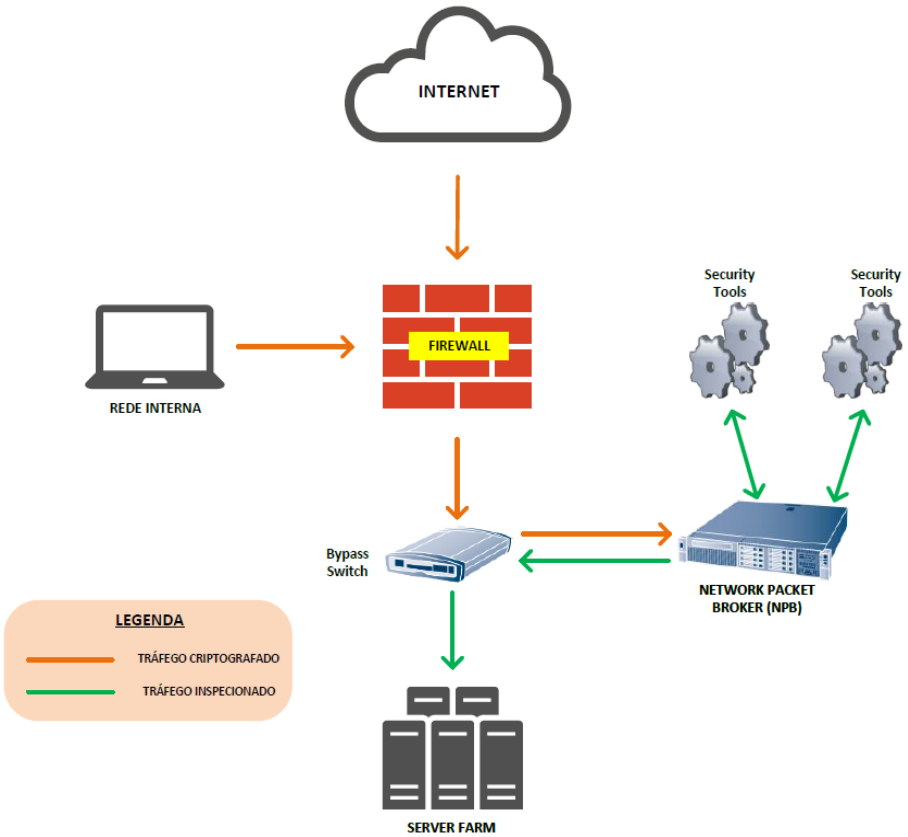

GESTÃO DE VULNERABILIDADES
CONTRATADA
CASA DA MOEDA (CMB)
AVALIAR (ASSESS)
PRIORIZAR (PRIORITIZE)
AGIR (ACT)
REAVALIAR (REASSESS)
MELHORAR (IMPROVE)
Realizar Identificação de Ativos
Início
Processo de Abertura de Chamados
Realizar Verificação de Vulnerabilidades
Demandar análise de Vulnerabilidades Específicas
Início
Relatório
Classificar e Ordenar as Vulnerabilidades
Elaborar Relatório de Correção das Vulnerabilidades
Aprovar Plano de Correção das Vulnerabilidades
Sim
Prazo Atingido?
Não
Documentar Aceitação ao Risco
Aprovado?
Não
Sim
Arquivar Risco
Sim
Não
Fim
Prazo Estipulado?
Resolver Problemas Identificados
Homologar Correção das Vulnerabilidades
Impacto Identificado?
Não
Sim
Avaliar Necessidade de Acionar Processo de Gestão de Mudanças
Relatório
Analisar Problemas/Erros Identificados
Impacto Identificado?
Sim
Não
Aplicar Correção das Vulnerabilidades em Produção
Viabilidade Técnica para Correção?
Sim
Não
Relatório
Elaborar Relatório de Inviabilidade de Correção e Realizar Rollback
Fim
Relatório
Reavaliar Vulnerabilidades
Correções bem Sucedidas?
Não
Sim
Relatório
Gerar Relatório de Acompanhamento do Processo de Gestão de Vulnerabilidades
Realizar Reunião de Encerramento
Avaliar Relatório e Aprovar Melhorias
Documentar e Implementar Melhorias
Sim
Aprovado?
Não
Fim

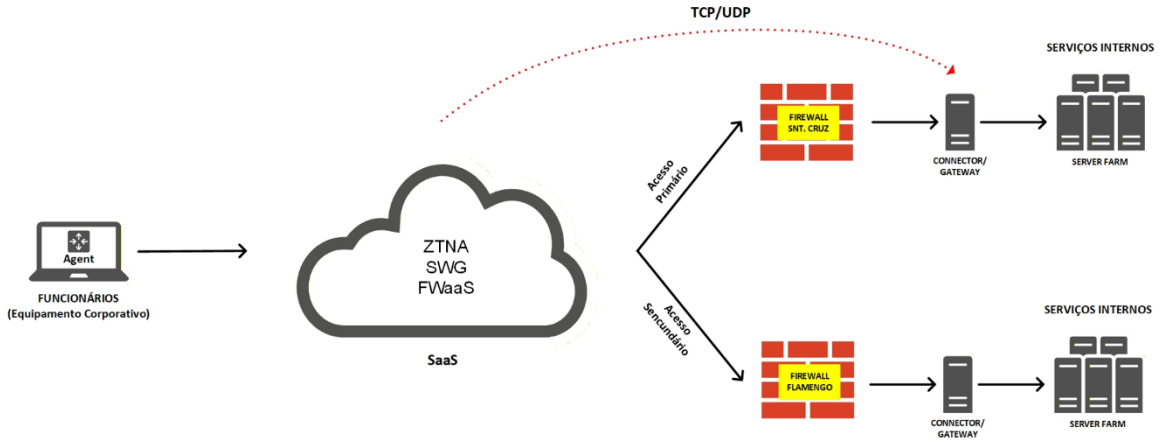
APENSO J – TOPOLOGIAS DE REFERÊNCIA

INCIDENT MANAGEMENT PLATFORM + NETWORK PACKET BROKER (NPB)

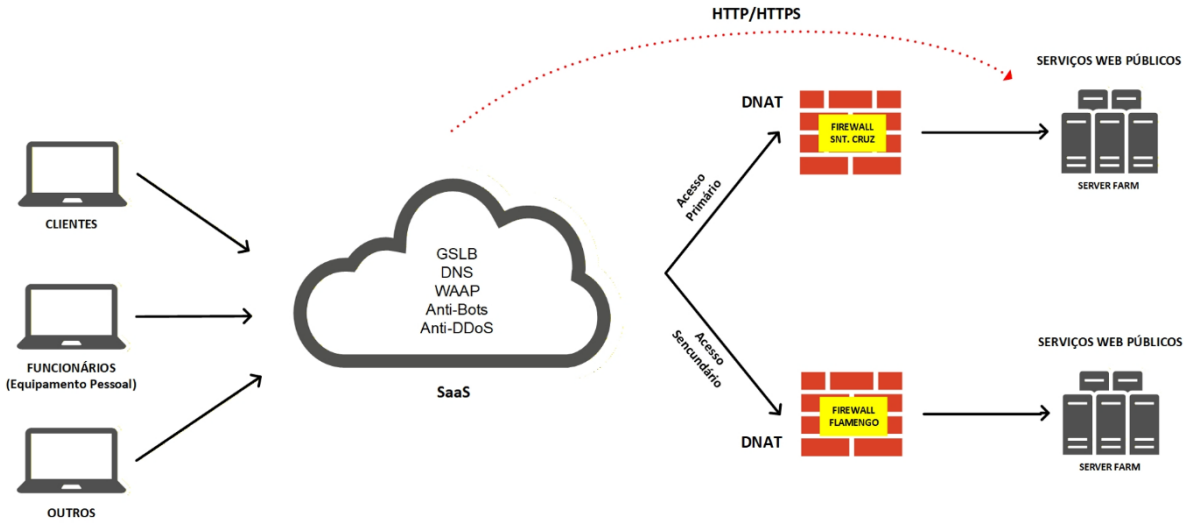



UNIDADE
SANTA CRUZ
UNIDADE
FLAMENGO
FIREWALL SNT. CRUZ
HA LINK
1G
Gb1
Gb2
Gb3
Gb4
20G
Bypass Switch
SWITCHES
GERÊNCIA
NETWORK PACKET BROKER (NPB)
APPLIANCE FÍSICO (TIPO I)
Coletor de log (Collector)
Análise do Tráfego (Sensor NDR)
Fiber TAP
Virtual TAP
FIREWALL FLAMENGO
LINK AGGREGATION
2G
APPLIANCE FÍSICO (TIPO II)
Coletor de log (Collector)
Análise do Tráfego (Sensor NDR)
LEGENDA
FIBRA ÓPTICA
COBRE (CAT 6)
FIBRA OUT-OF-BAND
COBRE OUT-OF-BAND
GRE TUNNEL

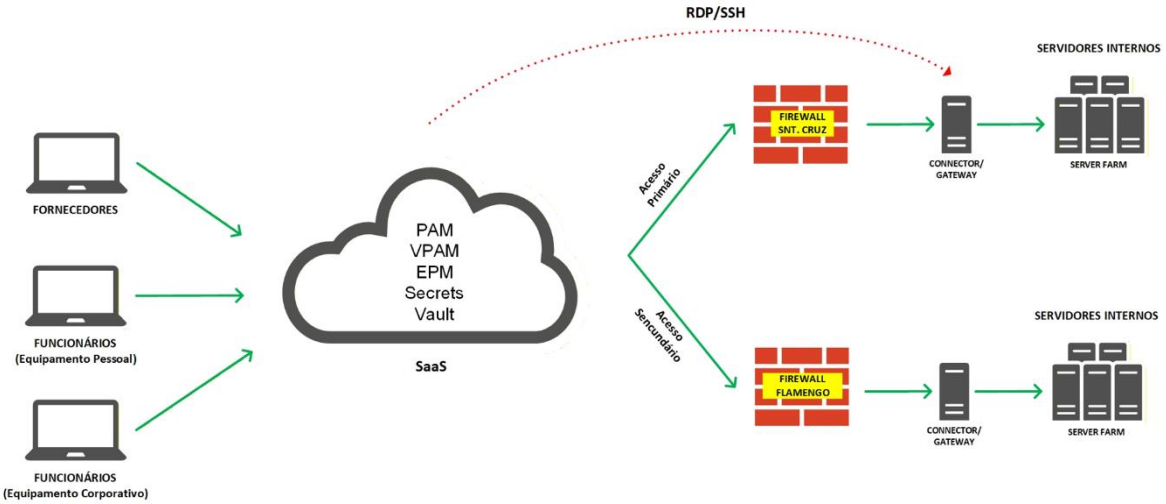

INTERNET
FIREWALL
REDE INTERNA
Security Tools
Security Tools
Bypass Switch
NETWORK PACKET BROKER (NPB)
SERVER FARM
LEGENDA
TRÁFEGO CRIPTOGRAFADO
TRÁFEGO INSPECIONADO



SECURITY SERVICE EDGE (SSE)



WEB APPLICATION SECURITY PLATFORM



UNIFIED IDENTITY SECURITY PLATFORM

ANEXO II

CLÁUSULAS E CONDIÇÕES PARA ELABORAÇÃO DA PROPOSTA

1. Fazer referência à presente licitação, com indicação do seu número de referência, em papel timbrado da licitante e, datada e assinada digitalmente (com certificado digital) pelo representante legal ou por procurador, devidamente identificado com números de CPF e RG, e respectivo cargo na licitante.
2. Não conter emendas, rasuras, entrelinhas e borrões, exceto se os mesmos forem devidamente ressalvados pelo PROPONENTE.
3. Apresentar validade de 60 (sessenta) dias consecutivos, contados a partir da data da abertura da sessão pública do pregão, caso a licitante não coloque a validade em sua proposta, será considerada como aceita a validade de 60 (sessenta) dias consecutivos.
4. Apresentar detalhadamente a descrição, o preço unitário e global dos serviços ofertados, conforme abaixo:

PLANILHA DE PREÇOS		
Item	**Descrição/Especificação**	**Total Mensal**
1	Serviço Gerenciado de Segurança (Managed Security Services - MSS) com Fornecimento de Soluções Tecnológicas de Cibersegurança	
TOTAL GLOBAL (36 MESES)		

4.1. Não serão admitidas, posteriormente, alegações de enganos, erros ou distrações na elaboração das propostas de preços.

5. Informar o prazo de entrega dos serviços, conforme Termo de Referência – ANEXO I, parte integrante deste Edital.
6. Nos preços ofertados já deverão estar incluídas todas as despesas com embalagem, tributos (federais, estaduais e municipais), transporte, encargos trabalhistas, previdenciários e comerciais e outras despesas de qualquer natureza que se fizerem necessárias ou indispensáveis à perfeita execução do objeto da licitação.

7. No mesmo documento ou à parte, sob as penas da lei, declarar a inexistência de impeditivos à contratação com a CMB, notadamente:

   7.1. em relação ao art. 38 da Lei n.º 13.303/2016:

      7.1.1. não possui administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social que seja diretor ou empregado da CMB ou de suas subsidiárias;

      7.1.2. não está cumprindo penalidade de suspensão temporária de participação em licitação e impedimento de contratar com a CMB;

      7.1.3. não foi declarada inidônea pela União, por Estado ou pelo Distrito Federal, enquanto perdurarem os efeitos da sanção;

      7.1.4. não possui sócio ou administrador que seja sócio de outra empresa que está suspensa, impedida ou declarada inidônea;

      7.1.5. não possui sócio ou administrador que tenha sido sócio ou administrador de outra empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção; e

      7.1.6. que não tem, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

   7.2. Em relação à Política de Transações com Partes Relacionadas (disponível em https://www.casadamoeda.gov.br/arquivos/lai/base-juridica/politica-de-transacoes-com-partes-relacionadas.pdf) declarar se é controlada ou não por:

      7.2.1. Superintendente, Diretor ou membro de Órgão previsto no estatuto social da CMB; ou por

      7.2.2. por cônjuge, companheiro ou parentes, consanguíneos ou afins, até o 3º grau, de qualquer pessoa referida na alínea (a) acima;

8. Condições de Pagamento: até 30 (trinta) dias consecutivos após apresentação da Nota Fiscal/Fatura.

9. Informações complementares tais como: razão social da licitante; CNPJ; endereço completo (inclusive CEP); telefone/e-mail; número da conta bancária; Banco/Praça; agência (código e nome).

DISCRIMINAÇÃO DOS VALORES						
Nome do Componente	**Fabricante**	**Part Number**	**Forma de Fornecimento**	**Qtde. (A)**	**Valor Unitário (B)**	**Valor Mensal (AxB)**
Incident Management Platform						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Network Packet Broker (NPB)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Cyber Threat Intelligence Platform (CTI)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Vulnerability Management Platform						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Breach and Attack Simulation (BAS)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						

Subtotal Mensal						
Next Generation Firewall (NGFW)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Secure Access Service Edge (SSE)						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Web Application Security Platform						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Unified Identity Security Platform						
Componente 1						
Componente 2						
Componente 3						
Componente n						
Serviço						
Subtotal Mensal						
Gerenciamento Soluções internas (PENSO H)						
Serviço						
Subtotal Mensal						

ANEXO III

MINUTA DE PROCURAÇÃO

OUTORGANTE: (nome, endereço, razão social, etc...)

OUTORGADO: (nome e qualificação do representante)

OBJETO: representar a outorgante perante a **CASA DA MOEDA DO BRASIL**

PODERES: apresentar PROPOSTA e DOCUMENTOS após o certame, prestar declaração de que o outorgante está em situação regular perante a Fazenda Nacional, Estadual e Municipal, Seguridade Social e o Fundo de Garantia do Tempo de Serviço – FGTS, bem como de que atende às exigências do Edital quanto à habilitação jurídica e qualificações técnica e econômico-financeira, formular ofertas e lances de preços nas sessões públicas, assinar as respectivas atas, registrar ocorrências, formular impugnações, interpor recursos, retirar Pedidos de Compra, assim como assinar todos e quaisquer documentos indispensáveis ao bom e fiel cumprimento do presente mandato.

LOCAL E DATA

ASSINATURA

ANEXO IV

MINUTA DO CONTRATO

TERMO DE CONTRATO Nº_____ QUE OBJETIVA A PRESTAÇÃO DE SERVIÇO GERENCIADO DE SEGURANÇA (MANAGED SECURITY SERVICES - MSS) COM FORNECIMENTO DE SOLUÇÕES TECNOLÓGICAS DE CIBERSEGURANÇA, QUE ENTRE SI FAZEM A **CASA DA MOEDA DO BRASIL - CMB** E A **#####.**

CASA DA MOEDA DO BRASIL - **CMB**, empresa pública, criada pela Lei nº 5.895, de 19/06/1973, com sede em Brasília (DF), estabelecimento fabril na Rua René Bittencourt nº 371, Distrito Industrial de Santa Cruz, Município do Rio de Janeiro, inscrita no CNPJ nº 34.164.319/0005-06, neste ato representada conforme seu Estatuto Social, doravante denominada **CMB** e **####**, estabelecida na (ENDEREÇO), inscrita no CNPJ sob o nº _____ , doravante denominada **CONTRATADA**, neste ato representada pelo seu (CARGO), Sr. (NOME), (qualificação do(s) representante(s) da **CONTRATADA**), tendo em vista o que consta no Processo nº 18750.002778/2025-01 e, em observância às disposições da Lei Federal nº 13.303, de 30 de junho de 2016 e Regulamento de Licitações e Contratos da CMB resolvem celebrar o presente Termo de Contrato, derivado do pregão eletrônico n° #####, mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente instrumento é a contratação de prestação de Serviço Gerenciado de Segurança (Managed Security Services - MSS) com fornecimento de soluções tecnológicas de cibersegurança, que será prestado nas condições estabelecidas no Termo de Referência – ANEXO I, parte integrante deste Contrato, assim como a proposta vencedora, independentemente de transcrição.

2. CLÁUSULA SEGUNDA – DA VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é de 36 (trinta e seis) meses, contados da assinatura do contrato, podendo ser prorrogado, até o limite previsto no art. 71 da Lei nº 13.303/2016, mediante acordo entre as partes.

2.1.1. O prazo de vigência poderá ser prorrogado, mediante justificativas, na hipótese de sobrevirem situações que impeçam ou prejudiquem a regular execução.

3. CLÁUSULA TERCEIRA – DO PREÇO E VALOR GLOBAL

3.1. O valor global do presente Termo de Contrato é de R$_____ (_____), conforme abaixo:

3.2. Nos valores acima estão incluídas todas as despesas com embalagem, tributos (federais, estaduais e municipais), transporte, encargos trabalhistas, previdenciários e comerciais e outras despesas de qualquer natureza que se fizerem necessárias ou indispensáveis à perfeita execução do objeto da contratação.

4. CLÁUSULA QUARTA – DO PAGAMENTO

4.1. O pagamento será efetuado pela CMB no prazo de 30 (trinta) dias consecutivos, contados da apresentação da Nota Fiscal/Fatura contendo o detalhamento do material entregue, através de transferência bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

4.2. Ocorrendo eventuais atrasos de pagamento, provocados exclusivamente pela CONTRATANTE, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 6% (seis por cento) ao ano, mediante a aplicação das seguintes fórmulas:

I = (TX /100) / 365

EM = I x N x VP

Onde:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

4.3. O pagamento somente será autorizado depois de efetuado o “atesto” pelo empregado competente na nota fiscal apresentada.

4.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CMB.

4.5. Será considerada data do pagamento o dia em que constar como emitida a transferência bancária para pagamento.

4.6. Antes do pagamento o gestor ou requisitante verificará a manutenção das condições de habilitação. Acaso existente irregularidade será concedido o prazo máximo de 05 (cinco) dias para a regularização ou apresentação da justificativa da impossibilidade de fazê-lo. Não havendo regularização ou sendo a justificativa considerada improcedente, a CMB deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

4.7. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente.

4.8. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

4.8.1. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123 de 2006, com as alterações da Lei Complementar n° 147 de 2014, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

4.9. Além de outras hipóteses previstas em lei ou no Contrato, a CMB poderá descontar, do montante expresso no documento fiscal ou equivalente legal, os valores referentes a multas e indenizações apuradas em processo administrativo, bem como qualquer obrigação que decorra do descumprimento da legislação pela CONTRATADA.

5. CLÁUSULA QUINTA – DOS RECURSOS ORÇAMENTÁRIOS

5.1. O recurso orçamentário destinado à cobertura da presente contratação será extraído do orçamento da CMB aprovado para os exercícios de 2026 a 2029, especificamente da rubrica “Serviços de Terceiros”.

5.2. No orçamento seguinte a **CMB** consignará os recursos necessários aos pagamentos previstos.

6. CLÁUSULA SEXTA – DO REAJUSTE

6.1. Desde que atendidos os requisitos básicos de qualidade e prazos estabelecidos no ANEXO I – Especificações de Serviços deste Contrato, os preços contratados poderão ser reajustados, com periodicidade anual, sendo o primeiro a contar de xx/xx/xxxx, data limite de apresentação da proposta, e os seguintes, do fato gerador anterior, com base em 90% (noventa por cento) da variação anual do IPCA (calculado e divulgado pelo IBGE), com base na seguinte fórmula:

$$PCr = PCb \times \{ 1 + [(((Vi\text{-}IPCA^{(n+11)}) / (Vi\text{-}IPCA^{(n-1)})) - 1) \times 0,9] \}$$, onde:

PCr = Preço Contratual reajustado;

PCb = Preço Contratual base;

$Vi\text{-}IPCA^{(n+11)}$ =Valor do nº Índice do IPCA do 11º (décimo primeiro) mês seguinte ao mês base Da data limite de apresentação da proposta;

$Vi\text{-}IPCA^{(n-1)}$ =Valor do nº Índice do IPCA do mês imediatamente anterior ao mês base da data limite de apresentação da proposta;

6.2. Compete a CONTRATADA apresentar o demonstrativo de cálculo referente ao pleito de reajuste anual de preços, destinada à CMB, conforme condições estabelecidas no caput desta cláusula.

6.3. O demonstrativo de cálculo referenciado no subitem anterior será encaminhado formalmente pela CONTRATADA ao Gestor do CONTRATO, mediante correspondência com confirmação de recebimento, que providenciará a verificação prévia e emitirá manifestação quanto à conformidade ou não da Contratada no atendimento aos requisitos básicos de qualidade e prazos estabelecidos no ANEXO I - Especificação de Serviços deste Contrato, que deverá ocorrer em até 05 (cinco) dias úteis a contar da data de apresentação e protocolo de recebimento da correspondência da Contratada na CMB;

6.4. Após manifestação prévia do Gestor do CONTRATO, este encaminhará imediatamente o pleito da CONTRATADA ao órgão financeiro da CMB responsável pela análise de cláusulas contratuais de reajuste de preços, que efetuará análise e emissão de pronunciamento técnico em 5 (cinco) dias úteis a contar da data de recebimento, pelo

órgão financeiro, da correspondência da Contratada contendo anexa a manifestação do Gestor do Contrato.

7. CLÁUSULA SÉTIMA – DA GARANTIA DE EXECUÇÃO

7.1. A CONTRATADA, no prazo de 45 (quarenta e cinco) dias após a assinatura do Termo de Contrato, prestará garantia no valor de R$.....(.....), correspondente a 3% (três por cento) do valor do total Contrato, que será liberada de acordo com as condições previstas neste Contrato, conforme disposto no art. 70 da Lei nº 13.303, de 2016, desde que cumpridas as obrigações contratuais. O prazo para apresentação da garantia poderá ser prorrogado por igual período a critério da CMB;

7.1.2 A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento);

7.1.3 O atraso superior a 25 (vinte e cinco) dias autoriza a CMB a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas.

7.2. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de mais 3 (três) meses após o término da vigência contratual;

7.3. Em caso de necessidade de apresentação da garantia, caberá à CONTRATADA optar por uma das seguintes modalidades de garantia:

7.3.1. caução em dinheiro;

7.3.2. seguro-garantia;

7.3.3. fiança bancária.

7.4. Optando pela modalidade fiança bancária, o instrumento de Fiança deverá prever a renúncia expressa, pelo fiador, ao benefício de ordem disposto no artigo 827 do Código Civil.

7.5. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

7.3.1 Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

7.3.2 Prejuízos causados à CMB ou a terceiro, independentemente de comprovação de culpa ou dolo, durante a execução do contrato;

7.3.3 As multas moratórias e punitivas aplicadas pela CMB à CONTRATADA;

7.3.4 Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela Contratada.

7.6. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior;

7.7. A garantia em dinheiro deverá ser efetuada em favor da CMB, no Banco do Brasil – Agência 3309-X - Conta Corrente 85001-2- código identificador CPF/CNPJ da contratada, informando à **Seção de Tesouraria - SETES** e será restituída com atualização monetária de acordo com a legislação aplicável;

7.8. Em caso de alteração do valor contratual, prorrogação do prazo de vigência do Contrato, utilização total ou parcial da garantia pagamento de qualquer obrigação ou em situações outras que impliquem em perda ou insuficiência da garantia, a CONTRATADA deverá providenciar a complementação ou substituição da garantia prestada no prazo a ser determinado pela CMB, não inferior a 05 (cinco) dias úteis, ou pactuado em aditivo ou em apostilamento, observadas as condições originais para aceitação da garantia estipuladas nesta Cláusula.

7.9. A CMB não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:

7.8.1 Caso fortuito ou força maior;

7.8.2 Descumprimento das obrigações pelo contratado decorrentes de atos ou fatos praticados pela CMB;

7.8.3 Atos ilícitos dolosos praticados por empregados da CMB.

7.10. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas nesta cláusula;

7.11. Será considerada extinta a garantia:

7.11.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CMB, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato.

8. CLÁUSULA OITAVA – DO REGIME DE EXECUÇÃO DOS SERVIÇOS E FISCALIZAÇÃO

8.1. Os serviços serão prestados sob regime de execução de empreitada por preço global.

8.2. Em cumprimento ao art. 40, VII c/c 69 da Lei nº 13.303, de 2016, o Superintendente do Departamento de TI Corporativo e Comunicação - DETIC da CMB designará representante, dando ciência à CONTRATADA mediante comunicação por correio eletrônico, para acompanhar e fiscalizar a entrega dos bens, anotando no processo de

acompanhamento todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

9. CLÁUSULA DÉCIMA - DAS OBRIGAÇÕES DA CMB

9.1. Autorizar o acesso da CONTRATADA às suas instalações, quando necessário em função do Contrato, desde que cumpridas as normas de segurança da CMB.

9.2. Fornecer todas as informações ou esclarecimentos e condições necessárias à plena execução do instrumento contratual.

9.3. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

9.4. Exercer o acompanhamento e a fiscalização dos serviços, por comissão ou empregado especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

9.5. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

9.6. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/empregado especialmente designado;

9.7. Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no presente Contrato e seus anexos;

9.8. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela contratada, quando for o caso.

9.9. Avaliar periodicamente a execução do contrato quanto a dados, materiais, documentos e informações de natureza sigilosa e exigir a assinatura de Termo de Confidencialidade do representante legal e dos profissionais envolvidos na execução sempre que estes tenham ou passem a ter acesso a informações sigilosas.

9.10. A CMB não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

10. CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA

10.1. A CONTRATADA deve cumprir todas as obrigações constantes no Contrato, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

11.1.1 Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções decorrentes da execução ou de materiais empregados, no prazo fixado neste Contrato e e/ou nos seus anexos.;

11.1.2 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

11.1.3 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto contratado em que se verificarem vícios, defeitos ou incorreções decorrentes da execução ou de materiais empregados, no prazo fixado neste Contrato e e/ou nos seus anexos.

11.1.4 Reparar todos os danos e prejuízos causados à CMB ou a terceiros, não restando excluída ou reduzida esta responsabilidade pela presença de fiscalização ou pelo acompanhamento da execução por parte do Gestor/Fiscal do Contrato.

11.1.5 Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

11.1.6 Observar e fazer observar, por seus empregados e prepostos, o disposto na legislação aplicável a prestação de serviços;

11.1.7 Indicar preposto para representá-la durante a vigência do Contrato;

11.1.8 Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

11.1.9 Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

11.1.10 Deter instalações, aparelhamento e pessoal técnico adequados e disponíveis para a realização do objeto da licitação;

11.1.11 Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

11.1.12 Manter, durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, comprovando-as sempre que solicitado pela CMB;

11.1.13 A CONTRATADA deverá se responsabilizar pela guarda e sigilo das informações da CMB que vier a ter acesso.

11.1.14 A CONTRATADA deverá certificar-se da adoção dos procedimentos necessários ao cumprimento da Lei nº 13.709/2018;

11.1.15 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos.

11.1.16 Não poderão beneficiar-se da condição de optante pelo Simples Nacional a microempresa ou empresa de pequeno porte que se enquadrar em alguma das situações previstas no art. 17, da Lei Complementar nº 123/06, salvo se dedicarem-se exclusivamente às atividades referidas nos §§5º-B a 5º-E do art. 18 desta Lei Complementar, ou as exerçam em conjunto com outras atividades que não tenham sido objeto de vedação no caput deste artigo;

11.1.17 A CONTRATADA deverá se submeter ao Acordo de Nível de Serviço – ANS e demais obrigações constantes do Anexo I – Termo de Referência.

11.1.18 A CONTRATADA, no prazo de 90 dias do início da vigência contratual, se compromete a adotar medidas eficazes, conforme suas políticas internas, para promover a equidade na ocupação das vagas, buscando, sempre que possível, a distribuição equilibrada entre homens e mulheres, bem como entre pessoas de diferentes raças e etnias.

12. CLÁUSULA DÉCIMA SEGUNDA - DA SUBCONTRATAÇÃO

12.1. Fica vedado neste ato, à CONTRATADA, transferir, ceder, subcontratar, negociar, utilizar em qualquer hipótese como garantia ou instrumento de fiança ou caução, seja comercial ou bancária, bem como transacionar com terceiros de qualquer personalidade jurídica, as obrigações, responsabilidades e demais CLÁUSULAS estabelecidas no presente Contrato, sem a competente, expressa e formal anuência da CMB.

13. CLÁUSULA DÉCIMA TERCEIRA – DA ANTICORRUPÇÃO, ÉTICA, CONDUTA E INTEGRIDADE

13.1. Na execução do presente Contrato é vedado à CMB e à CONTRATADA e a seus empregados, prepostos e gestores: a) prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público ou a quem quer que seja, ou a terceira pessoa a ele relacionada; b) criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o presente instrumento; c) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações do presente Contrato, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; d) manipular ou fraudar o equilíbrio econômico-financeiro do presente Contrato; ou e) de qualquer maneira fraudar o presente Contrato; assim como realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº 12.846/2013 e suas alterações, do Decreto nº 11.129/2022, ou de quaisquer outras leis ou regulamentos aplicáveis (“Leis Anticorrupção”), ainda que não relacionadas com o presente Contrato.

13.2. Além das disposições expressas neste contato, as partes pautarão o seu relacionamento na Integridade exigida nas relações público-privadas, rejeitando qualquer tipo de ação que resulte em vantagem indevida para agentes públicos e privados envolvidos, incluindo eventuais fornecedores, terceirizados ou quaisquer pessoas físicas ou jurídicas relacionadas com a cadeia de fornecimento do objeto deste contrato, assumindo pleno conhecimento e cumprimento das seguintes normas e orientações, além de outras eventualmente cabíveis:

- Lei Federal 13.303/2016 – Lei das Estatais;
- Lei Federal 12.846/2013 – Lei Anticorrupção;
- Decreto Federal 11.129/2022 - Regulamento da Lei Anticorrupção;
- Guia “Programa de Integridade – Diretrizes para Empresas Privadas” da Controladoria Geral da União (https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf)
- Código de Ética, Conduta e Integridade da Casa da Moeda do Brasil: (https://www.casadamoeda.gov.br/arquivos/pcmb/a-empresa/etica/codigo-de-etica/codigo-de-etica-cmb.pdf)
- Programa de Integridade da Casa da Moeda do Brasil: (https://www.casadamoeda.gov.br/arquivos/pcmb/transparencia/acesso-a-informacao/institucional/cartilha-programa-integridade.pdf).

13.1.1 Caso possua Programa de Integridade implementado, ainda que pautado em legislação estrangeira, a CONTRATADA o fornecerá para conhecimento da CMB.

13.1.2 A CONTRATADA concorda em submeter-se a ações de diligência promovidas pelas áreas de contratações e governança da CMB relativas ao cumprimento das normas e orientações acima relacionadas, colaborando com informações e documentos que sejam solicitados, voltados para o cumprimento do programa de integridade da CMB, resguardados os sigilos financeiros, empresariais e industriais que não se relacionem com o objeto do Contrato.

13.1.3 A CONTRATADA ou qualquer um de seus colaboradores denunciará à Ouvidoria da CMB, inclusive mediante os meios de proteção e preservação de identidade cabíveis, quaisquer condutas inadequadas - consumadas, tentadas ou propostas - relativas a vantagens ilícitas, fraudes ou qualquer prática de corrupção concernente ao relacionamento entre as partes deste contrato.

13.1.3.1 Reclamações e denúncias relativas a irregularidades ou ao descumprimento pela CMB de suas normas internas ou da legislação vigente durante a condução deste CONTRATO poderão ser apresentadas à Ouvidoria da CMB, por meio eletrônico (no endereço eletrônico www.casadamoeda.gov.br ou por meio de correio eletrônico ouvidoria@cmb.gov.br), por meio postal endereçado à Ouvidoria CMB na Rua René Bittencourt n° 371, Distrito Industrial de Santa Cruz, Rio de Janeiro/RJ ou pelo telefone (21) 2184-2969.

13.1.4 A CONTRATADA informará à CMB, com o detalhamento cabível, qualquer procedimento de responsabilização em decorrência de supostos atos de corrupção, no Brasil ou no exterior, que eventualmente venha a ser submetida em decorrência de legislação nacional ou estrangeira.

13.1.5 Casos de quebra de sigilo contratual ou qualquer outra hipótese de quebra de contrato, serão passíveis de indenização;

13.1.6 A transgressão a qualquer das disposições relativas ao cumprimento de normas e orientações de Integridade neste contrato e na respectiva legislação serão objeto de Processo Administrativo de Responsabilização – PAR, a ser instaurado pela CMB ou pela Controladoria-Geral da União – CGU, sem prejuízo das responsabilizações civis, penais e administrativas das pessoas físicas envolvidas em tais atos, bem como pela possibilidade de resolução contratual por responsabilidade do contratado.

14 CLÁUSULA DÉCIMA QUARTA – DA VEDAÇÃO AO NEPOTISMO

14.1 Nos termos do art. 7º do Decreto 7.203 de 2010, fica vedada, para prestar serviços na CMB, a contratação de cônjuge, companheiro ou de parente em linha reta ou colateral, por consanguinidade ou afinidade, até terceiro grau de servidor ocupante de cargo em comissão ou função de confiança, do quadro de pessoal da Contratante.

15 CLÁUSULA DÉCIMA QUINTA – DAS SANÇÕES ADMINISTRATIVAS

15.1 Comete infração administrativa, a CONTRATADA que:

15.1.1 inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

15.1.2 ensejar o retardamento da execução do objeto;

15.1.3 falhar ou fraudar na execução do Contrato;

15.1.4 comportar-se de modo inidôneo;

15.1.5 cometer fraude fiscal;

15.2 A CONTRATADA que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

15.2.1 advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a CMB;

15.2.2 multa moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite do valor total do contrato;

15.2.3 multa de até 10% (dez por cento) sobre o valor total do Contrato, no caso de inexecução total do objeto;

15.2.4 em caso de inexecução parcial, a multa, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

15.2.5 Suspensão temporária de participação em licitação e impedimento de contratar com a Casa da Moeda do Brasil por até 2 (dois) anos;

15.3 As penalidades de advertência e de suspensão temporária poderão ser aplicadas juntamente com a penalidade de multa.

15.4 Também ficam sujeitas às penalidades do art. 83, III da Lei nº 13.303, de 2016, a CONTRATADA que:

15.4.1 tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

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

15.4.3 demonstre não possuir idoneidade para contratar com a CMB em virtude de atos ilícitos praticados.

15.5 As sanções de caráter patrimonial observarão o valor limite do contrato.

15.6 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, conforme § 2º do art. 82 e § 2º do art. 83 da Lei n.º 13.303, de 2016.

15.7 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à CMB, observado o princípio da proporcionalidade.

15.8 Sem prejuízo da aplicação de penalidades, a CONTRATADA é responsável pelos danos causados à Administração ou a terceiros na forma disposta no artigo 76 da Lei 13.303, de 2016, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo órgão interessado.

15.9 As penalidades serão obrigatoriamente registradas no SICAF;

15.10 As multas previstas, quando aplicadas, deverão ser recolhidas na Seção de Tesouraria - SETES da CMB no prazo de até 10 (dez) dias úteis, contados do recebimento da notificação por correio ou outro meio qualquer, que ateste o recebimento.

15.10.1 Caso não haja recolhimento no prazo indicado no subitem acima e o valor da multa for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela diferença, a qual será descontada dos pagamentos eventualmente devidos pela CMB ou, ainda, quando for o caso, cobrada judicialmente, nos termos dos artigos 82, §§ 2º e 3 º e 83, § 1º, da Lei nº 13.303, de 2016.

15.11 Quando interposto, o recurso deverá ser entregue assinado digitalmente pelo representante da contratada ou seu procurador devidamente constituído, em até 10 (dez) dias úteis, contrarrecibo, ao Departamento de Contratações (DEGEC), que o receberá através da Seção de Emissão de Contratos (SEECT) pelo e-mail seect@cmb.gov.br.

16 CLÁUSULA DÉCIMA SEXTA – DA RESCISÃO

16.1 O presente Contrato poderá ser rescindido por acordo entre as partes, bem como nos demais casos legais.

16.2 Sem prejuízo da aplicação das sanções previstas, a CMB poderá rescindir o contrato na hipótese prevista no artigo 82, § 1º da Lei n° 13.303, de 2016, e na hipótese de inexecução total ou parcial do objeto.

16.3 Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito ao contraditório e ampla defesa.

17 CLÁUSULA DÉCIMA SÉTIMA – DAS VEDAÇÕES

17.1 É vedado à CONTRATADA:

17.1.1 transferir, ceder, negociar, utilizar em qualquer hipótese como garantia ou instrumento de fiança ou caução, seja comercial ou bancária, bem como transacionar com terceiros de qualquer personalidade jurídica, as obrigações, responsabilidades e demais **CLÁUSULAS** estabelecidas no presente Contrato, sem a competente, expressa e formal anuência da **CMB**.

17.1.2 interromper a execução contratual sob alegação de inadimplemento por parte da **CMB**, salvo nos casos previstos em lei.

18 CLÁUSULA DÉCIMA OITAVA – DAS ALTERAÇÕES

18.1 Eventuais alterações contratuais reger-se-ão pela disciplina do art. 81 da Lei nº 13.303, de 2016.

18.2 A CONTRATADA poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

18.3 As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

19 CLÁUSULA DÉCIMA NONA – DO MEIO AMBIENTE

19.1 A CONTRATADA deverá apresentar sua respectiva licença ambiental de operação compatível com a(s) atividade(s) solicitada(s) no edital, conforme o disposto no inciso III, artigo 8º da Resolução do Conselho Nacional do Meio Ambiente (CONAMA) Nº 237, de 19 de dezembro de 1997;

19.2 A construção, instalação, ampliação e funcionamento de estabelecimentos utilizadores e atividades utilizadoras de recursos ambientais, efetiva ou potencialmente poluidores ou capazes, sob qualquer forma, de causar degradação ambiental dependerão de prévio licenciamento ambiental, conforme artigo 10º da Lei Federal nº 6.938, de 31 de agosto de 1981;

19.3 Considera-se licenciamento ambiental o procedimento administrativo destinado a licenciar atividades ou empreendimentos que se utilizem de recursos ambientais, efetiva ou potencialmente poluidores ou capazes, sob qualquer forma, de causar degradação ambiental;

19.4 Cabe aos órgãos ambientais competentes (Órgãos Federal, Estadual ou Municipal) a definição das atividades descritas ou dos empreendimentos descritos no item acima, conforme incisos XIV dos artigos 7º, 8º e 9º da Lei Complementar nº 140, de 08 de dezembro de 2011;

19.5 Será obrigatória a apresentação das demais Certidões, Autorizações e Licenças previstas na legislação ambiental, que tenham a função de substituir a Licença de Operação, as quais deverão ter sido emitidas pelos órgãos ambientais competentes, conforme artigos 9º e 12 da Resolução CONAMA nº 237/1997;

19.6 A CONTRATADA que, conforme Legislações Ambientais Federal, Estadual e Municipal do local onde se encontra instalada, for enquadrada como isenta de licenciamento ambiental para as atividades realizadas pela empresa, deverá apresentar o(s) documento(s) emitido(s) pelo(s) órgão(s) ambiental(is) competentes(s) para comprovação de tal isenção.

19.7 Caberá à CMB realizar diligências para dirimir eventuais dúvidas.

20 CLÁUSULA VIGÉSIMA – DO SIGILO DAS INFORMAÇÕES E DA PROTEÇÃO A DADOS PESSOAIS

20.1 Caso a CONTRATADA venha a ter acesso a dados, materiais, documentos e informações de natureza sigilosa, direta ou indiretamente, em decorrência da execução do objeto contratual, deverá manter o sigilo dos mesmos, bem como orientar os profissionais envolvidos a cumprir esta obrigação, respeitando-se as diretrizes contidas nos normativos da CMB que orientam este assunto, em especial a POL-GOV.001 - Política de Proteção de Dados Pessoais (https://www.casadamoeda.gov.br/arquivos/lai/base-juridica/politica-de-protecao-de-dados-pessoais-e-divulgacao-de-informacoes.pdf), além da observância dos termos da Lei 12.527, de 18 de novembro de 2011 e da Lei 13.709, de 14 de agosto de 2018.

20.1.1 Sempre que solicitado pelo Gestor do Contrato, a CONTRATADA deverá providenciar a assinatura, por seu representante legal e pelos profissionais que tiverem acesso a informações sigilosas, dos Termos de Confidencialidade a serem disponibilizados pela CMB.

20.2 As PARTES devem estar em conformidade com a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 2018), assumindo toda e qualquer responsabilidade por violação à legislação de proteção de dados e privacidade nos tratamentos que eventualmente realizarem, diretamente ou por intermédio de outrem.

20.2.1 A CONTRATADA está ciente de que a CMB, em virtude da natureza de suas atividades, adota controles rígidos para acesso físico às suas unidades

industriais, abrangendo o tratamento de dados pessoais para verificações prévias e registros de acesso, inclusive mediante câmeras, e, se necessário, inspeção de cargas e pertences pessoais.

21 CLÁUSULA VIGÉSIMA PRIMEIRA – DOS CASOS OMISSOS

21.1 Os casos omissos serão decididos pela CMB, segundo as disposições contidas na Lei nº 13.303, de 2016, e demais normas federais de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

22 CLÁUSULA VIGÉSIMA SEGUNDA – DA PUBLICAÇÃO

22.1 Incumbirá à CMB providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União.

23 CLÁUSULA VIGÉSIMA TERCEIRA – DO FORO

23.1 O Foro para solucionar os litígios que decorrerem da execução deste Termo de Contrato será o da Seção Judiciária da Justiça Federal do Estado do Rio de Janeiro.

E, por estarem justos e acordados, firmam o presente instrumento em 1 (uma) via eletrônica, a qual, depois de lida, também é assinada eletronicamente para produzir seus jurídicos e legais efeitos, pelos representantes das partes, **CMB** e **CONTRATADA**:

CASA DA MOEDA DO BRASIL - CMB

CONTRATADA
