EDITAL DE CONSULTA PÚBLICA
CMB Nº 0001/2023

A Casa da Moeda do Brasil – CMB torna público que realizará Consulta Pública, **visando o aprimoramento do Termo de Referência** para contratação de empresa especializada para fornecimento de Plataforma Online para Conscientização em Segurança da Informação.

Data: 27 de julho de 2023
Horário: 10 horas.
Local: Sala Virtual do Microsoft Teams

Clique para ingressar na reunião

Condução: Departamento de Contratações – DEGEC e Departamento de Segurança – DESEG.

1. Do Objeto:

Contratação de empresa especializada para fornecimento de Plataforma Online para Conscientização em Segurança da Informação.

2. Do Objetivo:

2.1. Apresentar o Termo de Referência relativo ao objeto, franqueando a quaisquer interessados o acesso às informações pertinentes, a fazer contribuições e sugestões acerca do objeto, de modo que o futuro edital de pregão eletrônico permita a participação do maior número possível de interessados, com publicidade e transparência.

2.2. Importante ressaltar que os pregões eletrônicos na CMB são operacionalizados através do Portal de Compras do Governo Federal – https://www.gov.br/compras/pt-br/ . A participação das licitações estará condicionada ao prévio credenciamento no sistema.

3. Da Agenda da Consulta:

3.1. Programação

a) A partir das 09:45 horas – acesso dos participantes na sala virtual do MS Teams;
b) 09:50 – 10:00 horas Registro de Presença, com a ordenação dos inscritos para manifestação oral;
c) 10:00 – 10:30 horas Apresentação (leitura), das contribuições e sugestões recebidas na forma do subitem 5.2;
d) 10:30 – 11:30 horas Manifestação oral dos inscritos;
e) A partir das 11:30 horas - Elaboração e Leitura da Ata, com assinatura eletrônica dos todos os presentes;
f) Até 10:30 horas, a coordenação do evento aceitará eventuais contribuições e sugestões escritas pelos interessados.

3.2. Ressalvada a identificação de que trata a alínea “a”, os demais horários poderão ser modificados a exclusivo critério da coordenação do evento, objetivando-se dotar de racionalidade e eficiência os trabalhos, sem prejuízo dos objetivos da Consulta.

4. Forma de participação:

4.1. A Consulta Pública será aberta a todos os interessados, pessoas físicas nacionais ou estrangeiras que:

a) Representem pessoas jurídicas que tenham interesse no fornecimento do objeto do edital anexo, limitado a um representante por pessoa jurídica.

b) Acompanhem os representantes mencionados na alínea “a”.

4.1.1 Apenas a pessoa física eleita para representar a pessoa jurídica, limitado a um representante, poderá se inscrever para manifestações orais e será responsável perante a coordenação do evento para receber ulteriores correspondências e/ou comunicados.

4.2. As contribuições e sugestões poderão ser encaminhados previamente, com a devida identificação do proponente, em formulário próprio, anexado a este edital (Anexo IV), até às **12 horas** do dia **25/07/2023 (quinta-feira)**, pelo endereço eletrônico licitacoes@cmb.gov.br, sem qualquer prejuízo à formulação de nova manifestação oral ou escrita durante a Consulta.

4.3. As inscrições dos representantes para manifestação oral ou escrita serão recebidas apenas durante a realização da Consulta Pública e encerram-se às 10:00 h, na forma do item 3.1, alínea “b”.

4.4. Cada inscrito, obedecendo a ordem de inscrição, disporá de 15 (quinze) minutos para se manifestar, podendo reformular ou complementar sua manifestação no tempo adicional de 05 (cinco) minutos. Não serão permitidos apartes. A coordenação do evento e os Representantes da CMB poderão fazer perguntas aos inscritos para obtenção de esclarecimentos adicionais eventualmente necessários.

4.5. A coordenação do evento poderá interromper a palavra quando o inscrito extrapolar o tempo estabelecido no item 4.4, bem como nos casos em que o tema abordado não influir para o objetivo da Consulta Pública.

4.6. As contribuições e sugestões recebidas por escrito encaminhadas até às 12 horas do dia 25/07/2023 serão apresentadas durante a sessão pública, na medida da disponibilidade de tempo.

5. Da formulação das contribuições e sugestões:

5.1. As contribuições e sugestões, deverão ser encaminhadas de forma concisa e objetiva, com o preenchimento do Anexo IV do presente edital.

5.2. No preenchimento do Anexo IV, a proponente deverá identificar-se com o preenchimento completo das informações (Razão Social, CNPJ, tel., e-mail de contato) e descrever de forma concisa e objetiva, sempre que possível, identificando o tópico e/ou item ao qual pretende contribuir.

6. Da Consulta Pública:

6.1. A coordenação do evento poderá convocar quaisquer empregados que lhe convier, com a finalidade de melhor prestar os esclarecimentos técnicos, operacionais ou jurídicos pertinentes.

6.2. À coordenação do evento competirá dirimir as questões de ordem e decidir conclusivamente sobre os procedimentos adotados na Consulta. Para assegurar o bom andamento dos trabalhos, poderá conceder e cassar a palavra, além de determinar a retirada de pessoas que vierem a perturbar a Consulta.

7. Disposições Gerais:

7.1. Serão coibidas as condutas desrespeitosas ou com o fim de protelar ou desvirtuar o objetivo da Consulta.

Rio de Janeiro, 27 de junho de 2023.

Sérgio Eduardo da Silva Queiroz
Coordenador do Evento

ANEXO I

TERMO DE REFERÊNCIA

1. DO OBJETO

ITEM	CÓDIGO/ CMB	ESPECIFICAÇÃO	QTDE.	U.E.	CLASSE/ MAT
1	S10616	Contratação de empresa especializada para fornecimento de Plataforma *Online* para Conscientização em Segurança da Informação.	1	UN	6075

2. DA JUSTIFICATIVA

Descrição:
Essa contratação justifica-se pela necessidade de fomentar a cultura de Segurança da Informação dentro da Casa da Moeda do Brasil - CMB. Além da necessidade de se garantir a segurança de ativos de infraestrutura e de softwares, também há que se garantir a segurança através da camada humana. Isto porque a camada humana está constantemente sofrendo tentativas de Engenharia Social, que basicamente, consiste em uma técnica para enganar alvos (empregados sem treinamento em Segurança da Informação) se passando por pessoas ou empresas de confiança, para convencê-los a compartilharem informações sensíveis. Um dos principais tipos de ataque utilizando a engenharia social é o *Phishing* que utiliza mensagens fraudulentas ou maliciosas que simulam o contato de pessoas ou empresas conhecidas, seja através de site, *e-mail*, mensagens de texto, telefone, mídias sociais, entre outros meios, para obter informações e dados sigilosos. Portanto, o usuário, como o elo mais fraco para a segurança da informação, deve ser treinado para se comportar diante das diversas ameaças existentes. Para isso, a CMB busca contratar um serviço que promova experiências práticas, lúdicas e fundamentadas, capazes de facilitar a compreensão de um público diversificado. Ao despertar o interesse e promover a conscientização dos usuários, a CMB tornará seus colaboradores aptos para lidar com situações de risco de forma madura, possibilitando a criação de mais uma camada de segurança no ambiente.

3. DA MOTIVAÇÃO

Descrição:
A Casa da Moeda do Brasil - CMB é uma empresa pública federal, subordinada ao Ministério da Economia, que tem como missão prover e garantir soluções de segurança nos segmentos de meio circulante e pagamento, identificação, rastreabilidade, autenticidade, controle fiscal e postal. Assim sendo, a empresa é alvo frequente de tentativas de fraudes e ataques cibernéticos. Em função disso, bem como, da necessidade constante de aprimorar os seus processos, a CMB investe constantemente na capacitação do seu quadro funcional. Com esta contração, a empresa busca aprofundar o conhecimento de seus quase 2000 empregados em Segurança da Informação, visando aumentar a sua resiliência contra as constantes as ameaças existentes, inclusive no meio cibernético. Segundo o relatório *Data Breach Investigation Report 2022*, da *Verizon*, o elemento humano continua a ser o principal alvo de ataques nas organizações, correspondendo a 82% das violações. Além disso, a utilização de malwares e o roubo de credenciais fornecem os insumos necessários para um ataque social bem-sucedido, enfatizando a importância de mantermos um forte programa de conscientização de segurança. Nos últimos anos, a tecnologia de segurança da informação tornou-se um tema de máxima urgência, pois, à medida que a tecnologia evolui crescem também as ameaças à integridade, disponibilidade e confiabilidade dos dados produzidos, processados e administrados por pessoas, instituições e empresas.

Neste contexto, informações demonstram que o fator humano ainda é um dos principais impulsionadores das violações de segurança. Isso ocorre porque os atacantes muitas vezes usam táticas de engenharia social para manipular as pessoas e induzi-las a fornecer informações confidenciais ou executar ações que comprometam a segurança de uma organização.

Assim, a CMB busca por intermédio da contratação de uma empresa especializada para fornecimento de plataforma online de conscientização e sensibilização em segurança da informação, auxiliando ao programa de conscientização de segurança da CMB, mitigando riscos, fortalecendo a segurança dos dados tornando a organização mais preparada para lidar com ameaças externas e internas — erros dos usuários, Isso envolve educar os funcionários sobre as práticas recomendadas de segurança da informação, como usar senhas fortes, evitar clicar em links suspeitos e relatar atividades suspeitas imediatamente.

Embora o malware e as credenciais roubadas sejam uma preocupação significativa, eles muitas vezes são o resultado de um ataque social bem-sucedido. Portanto, combater esse tipo de ameaça começa com a conscientização e a educação dos empregados. Com um forte programa de conscientização em segurança da informação em vigor, ajuda a reduzir o risco de violações de segurança da informação causadas pelo fator humano.

Objetivo:

- A contratação é motivada pela necessidade de aprimorar o processo de conscientização e sensibilização em Segurança da Informação realizado na CMB, orientando todos os seus empregados quanto às ameaças que a empresa está sujeita;
- Aumentar o conhecimento dos empregados quanto às questões inerentes à Segurança da Informação, promovendo a mudança comportamental e aumentando o engajamento deles no combate às ameaças;
- Disponibilizar aos empregados conteúdos mais ricos e que se interliguem, proporcionando maior atratividade e interesse nas campanhas de conscientização e sensibilização em Segurança da Informação;
- Subsidiar a equipe responsável pela capacitação dos empregados no tema, com recursos adequados ao desenvolvimento de ações mais robustas e medições mais detalhadas;
- Informatizar e automatizar as diversas atividades do processo;
- Obter conteúdo em diversos formatos (Texto, imagem e vídeo), com suporte aos portadores de necessidades especiais, organizados de forma que auxiliem a criação de campanhas, aferição de resultados e acompanhamento da evolução individual dos empregados;
- Constituição e realização de campanhas.
- Elaborar gráficos adequados a necessidades do momento.
- Gamificação para incentivar a competição saudável entre os empregados.

Alinhamento Estratégico:

- A demanda está alinhada ao Planejamento Estratégico 2023 a 2027, atendendo ao seguinte objetivo estratégico: **"Manter a CMB alinhada às melhores práticas ambientais, sociais e de governança"**;
- Atende a iniciativa tática definida pelo DESEG para atendimento ao objetivo estratégico em questão: **"Implantar um Sistema de Gestão de Segurança da Informação (SGSI), baseado no guia da norma ABNT NBR ISO/IEC 27000)"**;
- O investimento também provisionado no **Orçamento DESEG 2023** aprovado pela Presidência;
- Por fim, a contratação também foi prevista no **Plano Anual de Contratações CMB – PAC 2023** (SEI Nº 18750.108488/2022-19).

4. CLASSIFICAÇÃO DOS BENS COMUNS

O objeto a ser contratado enquadra-se na categoria de bens comuns, de que se tratam a Lei nº 10.520/02, o Decreto nº 3.555/00 e o Decreto nº 10.024/19, por possuir padrões de desempenho e características gerais e específicas, usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da modalidade Pregão.

5. DO ENVIO DA PROPOSTA

A proposta deverá consignar:

- Todas as especificações do serviço ofertado de acordo com as especificações constantes deste Termo de Referência, inclusive marca e fabricante, quando houver, preços unitários e preço total, expressos em reais, incluindo todos os impostos, taxas, frete e demais encargos;

- O correio eletrônico, número de telefone para realização dos chamados, durante o período de vigência do instrumento contratual;

- Prazo de validade da proposta devendo ser de no mínimo 60 (sessenta) dias corridos.

6. DOS PAPÉIS E RESPONSABILIDADES

6.1. DAS OBRIGAÇÕES DA CMB

6.1.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos.

6.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo.

6.1.3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

6.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/empregado especialmente designado;

6.1.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no instrumento contratual e seus anexos;

6.1.6. 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;

6.1.7. Autorizar o acesso da CONTRATADA às suas instalações, quando necessário em função do instrumento contratual, desde que cumpridas as normas de segurança da CMB.

6.2. DAS OBRIGAÇÕES DA CONTRATADA

6.2.1. A Contratada deve cumprir todas as obrigações constantes no instrumento contratual, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

6.2.2. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no instrumento contratual e seus anexos, acompanhado da respectiva nota fiscal;

6.2.3. O objeto deve estar acompanhado do manual do usuário, com uma versão no idioma português (Brasil) e da relação da rede de assistência técnica autorizada, quando for o caso;

6.2.4. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

6.2.5. Substituir, reparar ou corrigir, às suas expensas, o objeto com avarias ou defeitos;

6.2.6. 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;

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

6.2.8. Indicar preposto para representá-la durante a execução do instrumento contratual, quando for o caso;

6.2.9. Enviar os certificados, laudos ou boletins técnicos que asseguram a qualidade dos itens classificados como garantidos pelo fornecedor, na data de entrega do mesmo, quando requeridos nas especificações técnicas de matérias-primas e insumos.

7. DA SUBCONTRATAÇÃO

É vedado 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.

8. CONTROLE DA EXECUÇÃO

8.1. Em cumprimento ao art. 40, VII c/c 69 da Lei nº 13.303/16, o Superintendente do Departamento DESEG da CMB designará representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

8.2. 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, de conformidade com o art. 76 da Lei nº 13.303/16.

8.3. O fiscal do contrato 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.

9. DAS SANÇÕES ADMINISTRATIVAS

9.1. Comete infração administrativa, a Contratada que:

9.1.1. Não executar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

9.1.2. Ensejar o retardamento da execução do objeto;

9.1.3. Fraudar na execução do contrato;

9.1.4. Comportar-se de modo inidôneo;

9.1.5. Cometer fraude fiscal;

9.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

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

9.2.2. 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;

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

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

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

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

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

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

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

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

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

9.7. 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.

9.8. 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 13.303/2016, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo órgão interessado.

9.9. As penalidades serão obrigatoriamente registradas no SICAF.

9.10. 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.

9.10.1. 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.

10. FORO DE ELEIÇÃO

Fica eleito o foro da Justiça Federal da Seção Judiciária do Estado do Rio de Janeiro (RJ) para a solução de questões oriundas deste instrumento.

11. QUALIFICAÇÃO TÉCNICA

Atestado(s) de capacidade técnica, expedido por pessoa(s) Jurídica(s) de direito público ou privado que, na condição de 01 (um) cliente(s) final(is), comprove(m) o fornecimento

satisfatório, pela licitante, de bens com características, quantidades e prazos compatíveis com o objeto da licitação.

11.1 Comprovação de capacidade técnica no fornecimento de suporte remoto e presencial:

11.1.1 Suporte e atendimento remoto e local de analistas de TI, cadastrados em uma única rede corporativa de um mesmo tomador de serviços, devendo essas informações constarem em um único atestado de capacidade técnica ou em mais de um atestado de capacidade técnica, desde que em período simultâneo igual ou inferior a 12 (doze) meses.

11.2 Para comprovação de capacidade técnica na execução da solução de conscientização em segurança da informação por meio de plataforma online:

11.2.1 Planejamento, instalação, configuração, monitoração, suporte e sustentação da solução de conscientização em segurança da informação por meio de plataforma online com operação em local adequado com regime de atendimento 24x7. O atestado deve indicar as marcas e modelos dos ativos e soluções administrados.

11.3 A declaração de capacidade técnica deve comprovar a experiência mínima de 6 (seis) meses na prestação dos serviços contratados.

11.4 Os atestados de capacidade técnica deverão referir-se a serviços prestados e/ou contratações realizadas no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

11.5 A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foram prestados os serviços, caso solicitado.

11.6 Somente serão aceitos atestados técnicos expedidos após a conclusão do contrato ou se decorrido, pelo menos, 1 (um) ano do início de sua execução.

11.7 Os atestados para comprovação da aptidão técnica para desempenho de atividades pertinentes e compatíveis em características e volume ao demandado pelo contratante deverão possuir conteúdo em que conste expressamente os serviços que foram executados pela empresa licitante, a sua “execução a contento” e sem ressalva, e os itens específicos a serem comprovados, devendo ainda ser emitidos em documento timbrado pela pessoa jurídica de direito público ou privado com a qual esta mantém (manteve) contrato de prestação de serviços, e deverá conter o nome, cargo ou função, dados de identificação (CPF e identidade), telefone e e-mail de contato do(s) seu(s) emissor(es), que possibilitem ao contratante, por intermédio de seu Pregoeiro, caso julgue necessário, confirmar sua veracidade junto ao cedente emissor.

11.8 Convém destacar que, na análise dos atestados de capacidade técnica, o contratante primará pela finalidade precípua da exigência, qual seja: a demonstração de que os licitantes possuem condições técnicas para executar o objeto pretendido pela Administração caso venha a sagrar-se vencedor da licitação. Assim, preservada a aderência aos ditames legais e constitucionais fundamentais, o exame documental balizar-se-á nos princípios da razoabilidade, da proporcionalidade e do formalismo moderado o que, por óbvio, não significa que serão admitidos quaisquer informalismos ou erros grosseiros.

11.9 A critério da CMB, poderá ser necessário diligenciar a pessoa jurídica indicada no Atestado de Capacidade Técnica, visando obter informações objetivas sobre o serviço prestado e/ou produtos entregues. Se for encontrada divergência entre o especificado nos atestados ou certificados de capacidade e o apurado em eventual diligência, além da desclassificação no presente processo licitatório, fica sujeita a licitante às penalidades cabíveis.

11.10 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 Termo de Referência.

12. DISPOSIÇÕES FINAIS

Havendo divergência entre as disposições deste Termo de Referência e o Edital, prevalecerão as do Edital.

ANEXO I – A

ESPECIFICAÇÃO DO SERVIÇO

1. OBJETO

O presente termo tem por objeto a contratação de empresa especializada para o fornecimento de solução de conscientização em segurança da informação por meio de plataforma online, que disponibilize conteúdos pré e pós concebidos, possibilitando a medição da absorção dos temas pelos praticantes, o desenvolvimento de campanhas com a criação de indicadores, a realização de simulações de ataques de engenharia social, incluindo os serviços de implantação, treinamento e suporte técnico da plataforma, nos termos e condições constantes no Edital e seus Anexos, durante toda a vigência da contratação.

2. ESCOPO DO SERVIÇO

2.1. A solução deve ser capaz de realizar, sem restrição de limites de uso, a comunicação, simulação de *Phishing*, treinamentos interativos atualizados periodicamente, campanhas de conscientização, boletins informativos, questionários e certificação do público-alvo sobre temas de Segurança da Informação e cibersegurança, minimamente, através das seguintes tecnologias: Mensagens eletrônicas através do *Microsoft Office 365 (Outlook e Teams), WhatsApp* e mensagens de texto para telefones celulares (SMS);

2.2. A solução deve ser capaz de atender todos os colaboradores da CMB, totalizando 2.000 (Duas Mil) pessoas, entre funcionários diretos, indiretos e/ou terceiros, chamados mais a frente, neste documento, de usuários-alvo.

2.3. A solução deverá permanecer ativa por 12 doze meses, ou seja, 1 (um) ano de contrato funcional com a CMB, podendo ser prorrogado por igual período ou maior, limitado a 60 meses.

2.4. Solução de conscientização em segurança da informação por meio de plataforma *online* de simulação de ataques de engenharia social na modalidade *Software* como Serviço (*"Software as a Service – SaaS"*).

2.5. A contratada deverá fornecer, durante o prazo de vigência do contrato, uma solução educativa que permita a simulação de *Phishing*, conforme requisitos definidos no Item 3 – Requisitos Básicos e Funcionais da Solução, incluindo garantia, manutenção e atualização do produto.

2.6. A solução deve ser desenhada especificamente para este fim, na qual não serão aceitas simulações executadas a partir dos *softwares* que não sejam concebidos especificamente para este fim.

2.7. O serviço deverá ser prestado pela CONTRATADA remotamente, e, caso a CONTRATADA necessite conectar no ambiente da CMB para tratar um problema no funcionamento da solução, a conexão deverá ser realizada por meio de VPNs (*Virtual Private Networks*), mediante autorização prévia, com definição de janela de serviço, garantindo sempre a confidencialidade, autenticação e integridade do tráfego de rede da CMB.

3. REQUISITOS BÁSICOS E FUNCIONAIS DA SOLUÇÃO

3.1. A solução não deve limitar a quantidade e/ou sofrer quaisquer alterações, inclusive de valor financeiro, com a alteração da quantidade de campanhas realizadas pela CMB.

3.2. A solução não deve limitar a quantidade e/ou sofrer quaisquer alterações, inclusive de valor financeiro, com a alteração da quantidade de modelos e ações das campanhas realizados pela CMB.

3.3. A solução deve ser capaz de realizar disparos das mensagens em períodos diversos, sejam eles: diários, semanais, quinzenais, mensais, trimestrais, semestrais, anuais e/ou de acordo com as necessidades da CMB, de forma independente, sem a obrigatoriedade de autorização do fabricante da plataforma e/ou prestador de serviços contratado.

3.4. A solução deve ser capaz de realizar agendamento automático e gestão (alterações e modificações) destes agendamentos via plataforma *web* de disparos das simulações em períodos diversos, sejam eles: diários, semanais, quinzenais, mensais, trimestrais, semestrais, anuais e/ou de acordo com as necessidades da CMB, sem a necessidade de autorização ou interação do fabricante da plataforma e/ou prestador de serviços contratado.

3.5. A solução deve possuir independência e não ser limitada pelo método de envio, tipo de mensagem simulada ou quantidade de envios, ou seja, podem ser realizados através de mensagens eletrônicas do *Microsoft Office 365 (outlook), Microsoft Teams, WhatsApp* e mensagens de texto para telefones celulares (SMS), sem distinção de uso e/ ou acréscimo financeiro.

3.6. A solução não deve limitar a quantidade e/ou sofrer quaisquer alterações, inclusive de valor financeiro, com a alteração da quantidade de contas de usuários-administradores que acessarão o painel de gerência da solução e que sejam colaboradores autorizados pela CMB.

3.7. A solução não deve limitar a quantidade e/ou sofrer quaisquer alterações, inclusive de valor financeiro, com a alteração da quantidade de localidades, servidores, processadores e/ou núcleos necessários da CMB.

3.8. A solução deve ser capaz de realizar os treinamentos e quaisquer outros tipos de ações, imediatamente após os usuários-alvo realizarem os acessos através das mensagens enviadas através do *Microsoft Office 365 (E-mail), Microsoft Teams, WhatsApp* e mensagens de texto para telefones celulares (SMS).

3.9. A solução deve ser capaz de registrar o aceite *online*, sobre documentos, políticas, treinamentos, códigos de ética, entre outros processos que exijam o aceite digital, através do *Microsoft Office 365 (E-mail), Microsoft Teams, WhatsApp* e mensagens de texto para telefones celulares (SMS), para todos os usuários-alvo.

3.10. A solução deve ser capaz de evidenciar que os usuários-alvo realizaram cada ação de uma campanha e/ou comunicado, através de um aceite formal dos mesmos, através do *Microsoft Office 365 (E-mail), Microsoft Teams, WhatsApp* e mensagens de texto para telefones celulares (SMS).

3.11. A solução deve ser capaz de realizar o encerramento, imediatamente após os usuários-alvo realizarem todas as ações de uma campanha realizada através do *Microsoft Office 365 (E-mail), Microsoft Teams, WhatsApp* e mensagens de texto para telefones celulares (SMS).

3.12. A solução deve permitir identificar quantos acessos únicos e totais cada usuário-alvo realizou em cada campanha e tipo de ação.

3.13. A solução deve possuir funcionalidade que automatize as campanhas e treinamentos, de forma a retirar ou incluir os usuários-alvos de acordo com a sua classificação (*ranking*) alcançada.

3.14. A solução deve reconhecer a origem do acesso e a rede que os usuários-alvo estão utilizando, incluindo provedor de serviços, domínio de acesso, País, Estado e/ou Cidade, nas interações com as campanhas através do *Microsoft Office 365 (E-mail), Microsoft Teams, WhatsApp* e mensagens de texto para telefones celulares (SMS).

3.15. A solução deve reconhecer o tipo de dispositivo e/ou aplicação que estão sendo utilizados pelos usuários-alvo, identificando sistema operacional, aplicação e/ou dispositivo, nas interações com as campanhas através do *Microsoft Office 365 (E-mail), Microsoft Teams, WhatsApp* e mensagens de texto para telefones celulares (SMS).

3.16. A solução deve possuir uma plataforma de questionários própria, bem como a possibilidade de integração com outras plataformas de questionário *online*, via API.

3.17. A solução deve permitir a realização de questionários (*quiz*) durante os treinamentos, em sua própria solução.

3.18. A solução deve permitir o envio de *Phishing* controlado, simulando propositalmente sites e aplicativos conhecidos no intuito de estimular o *click* dos usuários-alvo, consequentemente verificando a capacidade deles em identificar esse tipo de golpe.

3.19. A solução deve permitir múltiplas ações por campanhas, contemplando no mínimo as ações de Treinamento, Encerramento, Relatórios de Ameaças, Documentos, Políticas, Simulações e Comunicados.

3.20. A solução deve ser capaz de enviar campanhas de e-mails com anexos em *WORD* (arquivo.doc) para simulações que envolvam arquivos. Os registros devem contabilizar as aberturas dos *e-mails* e dos anexos de forma individual.

3.21. A solução deve permitir a criação de anexos *online* de forma fácil e intuitiva dentro de seu painel administrativo *web*, através de usuário-administrador autorizado pela CMB, sem a necessidade de interação do fabricante e/ou do prestador de serviços.

3.22. A solução não deve limitar a quantidade e/ou sofrer quaisquer alterações, inclusive de valor financeiro, com o uso e/ou alteração da quantidade de anexos a serem utilizados nas campanhas pela CMB.

3.23. A solução deve ser capaz de enviar lembretes automatizados para chamar a atenção dos usuários-alvo e lembrá-los de realizar treinamentos de campanhas anteriormente realizadas.

3.24. A solução deve permitir a criação de lembretes *online*, no que tange ao término de cada campanha de forma fácil, intuitiva e integrado ao seu painel administrativo *web*, através de usuário(s)-administrador(es) autorizado(s) pela CMB.

3.25. A solução não deve limitar a quantidade e/ou sofrer quaisquer alterações, inclusive de valor financeiro, com a alteração da quantidade de lembretes a serem utilizados nas campanhas pela CMB.

3.26. A solução deve permitir a utilização em qualquer dispositivo, seja um celular, *tablet* ou computador, e sua *interface* tem que ser responsiva ao tamanho da tela e tipo de dispositivo.

3.27. A solução deve permitir o funcionamento de múltiplas empresas no formato *multitenancy*, garantindo a segmentação dos dados e o acesso seguro as informações.

3.28. A solução deve permitir o gerenciamento de múltiplas empresas no formato *multitenancy* através de um único painel de administração.

3.29. A solução deve possuir o suporte do prestador de serviços contratado.

3.30. A solução pode possuir uma rede de parceiros qualificados para realizar a ativação, treinamento, execução e/ou suporte à sua plataforma, minimamente, no idioma português (Brasil).

3.31. A CONTRATADA deve possuir a lista de parceiros qualificados e acessíveis por qualquer empregado da CMB, através de seus contatos de comunicação, minimamente: *e-mail*, *site* e telefone.

3.32. A qualquer momento, durante a vigência do contrato, a CMB poderá efetuar a substituição de empregados ativos na plataforma por qualquer motivo da CONTRATANTE, logo o empregado excluído da plataforma não deverá mais ser contabilizado para fins de licenciamento.

3.33. A solução deve implementar módulo de simulação de *Phishing*, todos no mesmo *software*, composto de no mínimo:

3.33.1. Módulo de construção de e-mail para simulação de *Phishing*;

3.33.2. Módulo de conscientização educacional de reconhecimento de *Phishing*;

3.33.3. Módulo gráfico e de relatórios que permita avaliar se o usuário reportou à área de segurança o possível *Phishing* sofrido.

3.34. Todas as atividades da CONTRATADA que envolvam usuários do CONTRATANTE deverão ser realizadas no idioma português (Brasil), incluindo todos os níveis de atendimento, material fornecido, *sites* e conteúdos disponibilizados, pesquisas de satisfação, mensagens, entre outros.

3.35. A solução fornecida não deve ter limites quanto à quantidade de disparos de *Phishing* dentro do período de contrato.

3.36. A solução deve possuir domínios personalizados de ataque prontos para sua simulação.

3.37. A solução deve possuir sua própria estrutura de envio de *e-mails* (Servidor SMTP), não onerando os recursos da CMB para o envio dos *e-mails* de simulação.

3.38. A solução deve fornecer páginas de destino (*landing page*) minimamente, no idioma português (Brasil), personalizáveis para cada modelo de simulação, podendo serem elas uma revisão do *Phishing*, uma página de erro, uma notificação sobre o programa de conscientização ou mesmo uma página personalizada de simulação de coleta de credenciais.

3.39. A solução deve fornecer rastreamento de resposta de *Phishing* que permita ao administrador saber quando um usuário tentar responder um *e-mail* de *Phishing* simulado.

3.40. A solução deve possuir suporte a inserção de usuários em lote através de arquivo CSV ou similar, permitindo ainda a separação dos usuários em grupos específicos.

3.41. A solução permitir a integração com o *Azure Active Directory (Azure AD)* para fazer o *upload* de dados dos usuários, eliminando a necessidade de gerenciar manualmente as alterações dos usuários.

3.42. A solução deve possibilitar, na visão do usuário atacado, a inserção de seus dados, porém, esses dados não devem ser armazenados de nenhuma forma em bases internas da solução ou bases externas.

3.43. A solução deve permitir a criação de *templates* personalizados para a CMB, onde seja possível definir modelos por departamentos, minimamente, no idioma português (Brasil), com a logo marca da CMB, contendo ao menos as seguintes opções:

3.43.1. Customização do nome e extensão de um anexo do e-mail de simulação de *Phishing*;

3.43.2. Seleção de usuário e de grupo de usuários que farão parte da simulação;

3.43.3. Seleção de agendamento com data e horário para início e fim de cada campanha de conscientização, específica por grupo a ser atingido.

3.43.4. Definição do nome do remetente que enviará o *e-mail* de simulação do *Phishing*;

3.43.5. Definição de assunto do e-mail de simulação do *Phishing*;

3.43.6. Definição do endereço (usuário e domínio) do *e-mail* de simulação do *Phishing*;

3.44. A solução deve possibilitar o uso de variáveis de ambiente, que permitam incluir individualmente no corpo do *e-mail* conteúdos dinâmicos, para no mínimo:

3.44.1. Nome do usuário;

3.44.2. Sobrenome;

3.44.3. Endereço de *e-mail*;

3.44.4. Nome da empresa;

3.44.5. Dia, Data, Hora, Ano.

3.45. A solução deve disponibilizar plataforma para configuração de campanhas de treinamento automatizadas com *e-mails* de lembrete agendados:

3.45.1. Possibilidade de selecionar módulos de treinamento por grupos de usuários;

3.45.2. Possibilidade de atribuir automaticamente treinamentos a novos usuários;

3.45.3. Possibilidade de configurar disparo automático de *e-mails* lembrete para usuários com treinamentos pendentes.

3.46. A solução deve fornecer acesso ilimitado a biblioteca com o seguinte conteúdo:

3.46.1. Módulos de Treinamento;

3.46.2. *Games* (Jogos);

3.46.3. Módulos de Vídeo;

3.46.4. Documentos e *Newsletters*;

3.46.5. Artes e Posteres;

3.46.6. *Assessments* (Pesquisas de avaliação).

3.47. A solução deve disponibilizar recursos que estimulem os participantes a avaliarem seus conhecimentos, seja através de perguntas em *quizzes* (questionários rápidos), seja através da tomada de decisões em ambientes que simulam suas atividades cotidianas, incluindo *feedback* imediato para as respostas e escolhas do colaborador.

3.48. A solução deve disponibilizar recursos lúdicos, que permitam aos usuários competir com seus colegas em placares de líderes e ganhar emblemas ao mesmo tempo em que aprendem.

3.49. A solução deve disponibilizar um catálogo de treinamentos voltados para a conscientização em Segurança da informação.

3.50. A solução deve ofertar boletins informativos atuais sobre “Golpe da semana”, “Dicas de segurança” e “Datas Comemorativas de assuntos de segurança da informação conforme calendário anual” visando manter os usuários participantes informados sobre os golpes de segurança da informação mais recentes e reforçar as dicas de segurança básica.

3.51. A solução deve possibilitar ofertar conteúdos por nível de proficiência, do básico ao avançado, passando pelo intermediário.

3.52. A solução dever possuir ao menos 200 (duzentos) vídeos dublados e legendados simultaneamente sincronizados, minimamente no idioma português (Brasil) e no formato *MP4* com resolução mínima de 720p, mas que também possam ser visualizados via *browser*, relacionado a temas de segurança da informação atualizados periodicamente, tais como:

3.52.1. Tipos de Ataque (Ex.: Engenharia social, *Malwares*, *Phishing*, Smishing, Ransomware, Negação de Serviço, etc.)

3.52.2. Uso seguro da *Internet* (Ex.: Senhas, *E-mail*, Mídias sociais, Privacidade de dados, Realização do trabalho à distância,

3.52.3. Boas Práticas de Segurança (Ex.: Utilização de redes sem fio, Dispositivos USB, Dispositivos móveis, Tela e mesa limpa, etc.)

3.52.4. Legislação e Conformidade (Normativos da CMB, Lei Geral de Proteção de Dados Pessoais – LGPD, NBR ISO 27001, Lei de Acesso à Informação, etc.)

3.52.5. Outros (Reporte de incidentes, Segurança física, Segurança pessoal, etc.)

3.53. A solução deve ter a capacidade de enviar uma mensagem a cada usuário participante da campanha que tenha clicado no *Phishing*, informando da campanha e os próximos procedimentos a serem adotados.

3.54. A solução deve ser capaz de apresentar de forma gráfica o progresso na conscientização dos usuários, executando gráficos comparativos entre campanhas já realizadas pela ferramenta, onde poderá ser observado o declínio e a ascensão na maturidade e conscientização da CMB.

3.55. A solução deve ser capaz de criar relatórios executivos e mostrar de forma gráfica na console do produto, no mínimo:

3.55.1. Verificação de quantos usuários inseriram os dados solicitados no e-mail de simulação de *Phishing*;

3.55.2. Verificação de quantos usuários identificaram e reportaram a simulação de *Phishing*;

3.55.3. Verificação de quantos usuários executaram o módulo de conscientização educacional Anti-*Phishing*;

3.55.4. Verificação da geolocalização dos usuários que sofreram a simulação do ataque de *Phishing* e foram capturados na simulação.

3.56. A solução deve apresentar de forma gráfica o resultado geográfico de qual localidade o *e-mail* de simulação do ataque *Phishing* foi efetivo com usuários que foram envolvidos na simulação.

3.57. A solução deve permitir a extração de todos os relatórios apresentados através de arquivo CSV editável ou similar.

3.58. A solução deve permitir avaliar os níveis de risco do usuário, de determinados grupos e de níveis organizacionais, de modo que o administrador tome decisões baseadas em dados.

3.59. A solução deve disponibilizar ambiente de gestão para acompanhamento *online* da progressão e desempenho dos participantes.

3.60. A solução deve disponibilizar relatórios avançados, executivos e de gestão, sobre as campanhas e resultados de treinamentos, com possibilidade de personalização e integração com ferramentas de BI.

3.61. A solução deve permitir que se analise em tempo real como os usuários estão se saindo de forma individualizada em comparação às outras empresas do mercado (*Benchmarking*).

3.62. A solução deve disponibilizar perfis de acesso (*security roles*) que permitam configurar permissões por usuários e grupos, para fins de gestão de resultados, gestão de campanhas de treinamento e auditoria.

3.63. A solução deve possibilitar a criação de grupos de usuários, baseados no comportamento frente as simulações, treinamentos e atribuições de cada colaborador para personalizar e automatizar as campanhas de aprendizagem e os relatórios de grupos de usuários.

3.64. A solução deve disponibilizar recurso de inativar usuários na plataforma sem prejuízo ao histórico de dados de treinamento destes usuários.

3.65. A solução deverá disponibilizar recurso que permita criar de maneira automatizada um programa de conscientização de segurança personalizado. A solução deve permitir aos usuários responderem questionários diretamente na plataforma.

3.66. A solução deve permitir o acompanhamento de todas as respostas dos questionários diretamente na plataforma *online*, bem como através de relatórios e via API.

3.67. A solução deve permitir dar o aceite *online* em documentos, políticas e termos diretamente na plataforma.

3.68. A solução deve permitir simular páginas e sistemas falsos, coletando as respostas enviadas pelos usuários.

3.69. A solução deve permitir quaisquer quantidades de ações em uma campanha, por exemplo, treinamentos, questionários, documentos e simulações, sem ordem específica.

3.70. A solução deve permitir múltiplas ações de um mesmo tipo, por exemplo vários treinamentos ou documentos, permitindo modelos modulares que possam ser reutilizáveis.

3.71. A solução deve permitir o encerramento e/ou encaminhamento dos usuários-alvo imediatamente, durante e/ou ao final do treinamento.

3.72. A solução deve permitir acompanhar, visualizar e exportar todas as entregas de mensagens realizadas com ou sem sucesso, categorizando e detalhando cada etapa do processo, através da plataforma *online*, relatórios e API.

3.73. A solução deve possuir módulo dedicado a pesquisa de satisfação, onde será possível determinar melhorias no aprendizado, métricas de segurança e de referência, bem como lacunas no conhecimento, capturar opinião de um coletivo ou individualmente dos participantes.

3.74. A solução deve possuir ferramenta para criar programa de conscientização e sensibilização em SI se baseando pelo calendário, com isso automatizando as ações.

3.75. A solução deve possuir painel de visualização a porcentagem de usuários que fatalmente irão cair em um *phishing* em comparação com a concorrência bem como o nível de risco geral da contratada.

3.76. A solução deve ser capaz de selecionar automaticamente o modelo de simulação de *phishing* para cada um dos participantes com base no histórico do usuário.

4. MODELOS (TEMPLATES) CONTEMPLADOS PELA SOLUÇÃO

4.1. A solução deve possuir modelos (templates) de ações de treinamentos no padrão scorm (padrão internacional para cursos *online*), comunicados, simulações, questionários, documentos e políticas com conteúdo focado nos tipos de mensagens e/ou campanhas que forem utilizadas para os usuários-alvo, através do *Microsoft Office* 365 (*outlook*), *Microsoft Teams*, *WhatsApp* e mensagens de texto para telefones celulares (SMS).

4.2. A solução deve conter modelos de agradecimentos que permitam a inserção de *links* para outros conteúdos online disponibilizados pela CMB ou terceiros.

4.3. A solução deve possuir modelos de mensagem de *Phishing* com contadores de tempo.

4.4. A solução deve possuir no mínimo 1.000 (um mil) modelos completos de mensagens, comunicados, campanhas e/ou treinamentos.

4.5. A solução deve permitir criar e editar todo conteúdo dos modelos, sem obrigatoriamente ter ajuda de terceiros.

4.6. A solução deve possuir modelos de mensagens, treinamentos e encerramentos, minimamente, no idioma português (Brasil).

4.7. A solução deve permitir o desenvolvimento de modelos futuros de mensagens, comunicados, documentos, questionários, simulações, treinamentos e encerramentos no idioma português (Brasil) e direto na plataforma online por qualquer usuário com o devido perfil de acesso.

4.8. A solução deve possuir todos os modelos acessíveis via *website* através da plataforma.

4.9. A solução deve possuir no mínimo 50 (cinquenta) modelos de ações para serem usadas nas campanhas, incluindo de treinamentos, questionários, documentos e simulações, minimamente, no idioma português (Brasil).

4.10. A solução deve permitir a criação e edição *online* de modelos de campanhas, mensagens de simulações, treinamentos e agradecimentos, através do seu próprio portal de aplicação *web*, sem a obrigatoriedade do uso de ferramentas de terceiros.

4.11. A solução deve possuir editor *online* interativo de campanhas e treinamentos simplificado, preferencialmente a do tipo WYSIWYG (*What You See Is What You Get* - "O que você vê é o que você obtém"), seguindo melhores práticas do mercado de *Cybersecurity* e de usabilidade.

4.12. A solução deve permitir o teste ilimitado para validação, em ambiente de homologação e laboratório, de campanhas, para até 10 (dez) usuários-alvo cadastrados para o fim, sem a ocorrência de consumo de disparos e de forma automatizada.

5. REPORTE E ANÁLISE DE AMEAÇAS ORIUNDAS DA SOLUÇÃO

5.1. A solução deve permitir integração nativa com as plataformas Microsoft (*Microsoft Office* 365 e *Microsoft Teams*), *WhatsApp* e mensagens de texto para telefones celulares (SMS) que permitam aos usuários interagir e relatar mensagens suspeitas e simuladas ao CSIRT CMB, para analisar e prevenir qualquer ameaça de *Phishing*, realizar a coleta de informações e analisar outras ameaças cibernéticas.

5.2. A solução deve contemplar a capacidade de reportar ameaças através das plataformas *Microsoft Teams* (*Office 365 e Outlook*), O relato deve estar disponível *online*, juntamente com a mensagem em anexo, além de todas as informações disponíveis, para a correta análise dos times responsáveis na CMB.

6. DASHBOARDS ANALYTICS E RELATÓRIOS ONLINE DA SOLUÇÃO

6.1. A solução deve possuir *dashboards analytics* e relatórios *online* que contemplem os dados abaixo, no mínimo:

6.1.1. Total de Mensagens: Campanha, Domínios, Etiquetas, Tipos de Mensagens e Pessoas.

6.1.2. Mensagens totais: Enviadas, Abertas e por ação das campanhas.

6.1.3. Pessoas únicas: Enviadas, Abertas e por ação das campanhas.

6.1.4. Dispositivos: Sistemas, Aplicações e Dispositivos, com detalhes de Bloco Econômico, País, Estado, Cidade, bem como Sistema Operacional, Aplicação, versão e tipo do dispositivo.

6.1.5. Todos os *dashboards analytics* e relatórios *online*, exportáveis ou via API podem ser filtrados por qualquer informação disponível dos contatos, como departamento, unidade de negócios, tempo de trabalho, gênero e etc.

6.2. A solução deve possuir *dashboards analytics* e relatórios *online* com georreferencia e mapas.

6.3. A solução deve ser capaz de realizar o acompanhamento dos resultados de forma 100% *online* e acessível via *website* da própria solução, exportáveis para documentos e acessíveis através de API documentada e disponibilizada pela própria solução.

6.4. A solução deve permitir a visualização de resultados através de empresas, departamentos, campanhas, gêneros, cargo, unidades de negócio, localidade, idade, tempo de empresa, nomes das pessoas e quaisquer outros tipos de informações disponíveis de cada pessoa.

6.5. A solução deve possuir módulo de *dashboards analytics* e relatórios *online* para acompanhamento e mensuração de todos os resultados, incluindo quantos usuários-alvo abriram, clicaram, treinaram, reportaram, além de todo e qualquer

outro tipo de ação individual registrável possível. Os registros devem informar a quantidade de vezes que cada usuário-alvo fez uma determinada ação de forma quantitativa e qualitativa.

6.6. A solução deve permitir a visualização de resultados através de mapas e georreferencia *global*, com detalhes por País, Estados e Municípios. Todos os registros de georreferencia devem ser exportáveis.

6.7. A solução deve ser capaz de exportar todo e qualquer dado incluído ou resultado de processamentos, através de uma *interface* intuitiva e de fácil acesso, com apenas um clique.

6.8. A solução deve possuir painéis e indicadores dinâmicos, onde possibilite a filtragem dos dados.

6.9. A solução deve informar os indicadores com dados quantitativos das campanhas, em números totais e qualitativos e em percentual sobre o todo, diretamente do seu painel principal (*dashboard*).

6.10. A solução deve possuir dashboards analytics e relatórios online com o histórico de campanhas e treinamentos por empresa, departamento, navegadores, gênero, idade, tempo no cargo, localidade, unidade de negócio, função, pessoas e quaisquer outras informações disponíveis de cada contato.

6.11. A solução deve possuir *dashboards analytics* e relatórios online que identifiquem ações individuais e totais de vezes que os usuários-alvo interagiram na mesma campanha, com indicadores únicos para envios, abertura, e por ações das campanhas, como treinamento, documentos, política, simulações, dentre outras.

6.12. A solução deve possuir *dashboards analytics* e relatórios *online* que identifiquem o comportamento e duração das campanhas.

6.13. A solução deve possuir *dashboards analytics* e relatórios *online* que usem de *gamification* (disputa lúdica via pontuação), atribuindo pontos de acordo com as ações dos usuários-alvo no decorrer das campanhas.

6.14. A solução deve possuir *dashboards analytics* e relatórios *online* de segurança com todas as origens, aplicações e IPs de acesso.

6.15. A solução deve disponibilizar todos os *dashboards analytics* e relatórios *online* com permissão através de perfis de acesso de usuários-administradores.

6.16. A solução deve disponibilizar todos os *dashboards analytics* e relatórios *online* através de aplicativo.

6.17. A solução deve disponibilizar a exportação de todos os *dashboards analytics* (dinâmicos e estatísticos), todos os tipos de relatórios *online*, minimamente, nos formatos XLSX, CSV, JSON e PDF.

6.18. A solução deve disponibilizar todos os dados através de API ou através de acesso ao banco de dados da solução, com acesso somente de leitura, minimamente.

6.19. A solução deve possuir a capacidade de disponibilizar todos os *dashboards*, estatísticas, relatórios e outros dados para a CMB através de integração, aplicativo e/ou envio de dados para plataformas de SIEM.

6.20. A solução deve possuir dashboards, estatísticas e relatórios *online* dos últimos 12 (doze) meses de *benchmarking* (comparativos), contemplando os resultados do ambiente da CMB, com os resultados globais da solução.

6.21. A solução deve possuir *dashboards*, estatísticas e relatórios *online* do consumo e validade deste CONTRATO informando linha de tempo, percentuais e quantidade utilizada da assinatura contratada.

6.22. A solução deve possuir *dashboards*, estatísticas e relatórios online comparativos com outros ambientes e com o histórico *global* da solução, contemplando as médias de envios, abertura, cliques e treinamentos.

7. PROVISIONAMENTO DE USUÁRIOS-ALVO, USUÁRIOS-ADMINISTRADORES E USUÁRIOS-APROVADORES

7.1. A solução deve possuir mapeamento de todos os perfis e jornadas dos usuários principais: Usuários-Administradores, Usuários-Aprovadores e Usuários-Alvo (colaboradores).

7.2. A solução deve suportar o provisionamento *online* de Usuários-Administradores, Usuários-Aprovadores e Usuários-Alvo (colaboradores), através de seção *online* destinada a esta função.

7.3. A solução deve suportar o provisionamento de Usuários-Administradores, Usuários-Aprovadores e Usuários-Alvo (colaboradores), através de API destinada a esta função.

7.4. A solução não deve ter limites ou sofrer alterações de valor por contas de Usuários-Administradores cadastrados para acesso e manipulação da solução.

7.5. A solução deve possuir a capacidade de criação de perfis: Usuários-Administradores, Usuários-Aprovadores e Usuários-Alvo (colaboradores);

7.6. O perfil Usuário-Administrador deve ser o grupo com maior privilégio da solução, permitindo a ele definir o tipo de acesso dos demais perfis às funcionalidades e informações do sistema.

7.7. A solução deve permitir a revogação de acesso de Usuários-Administradores a qualquer momento através da plataforma *online* ou via API.

7.8. A solução deve permitir automatizar a atualização de Usuários-Administradores, Usuários-Aprovadores e Usuários-Alvo (colaboradores), direto dos sistemas internos, como o *Azure Active Directory* (*Azure AD*), através da API.

7.9. A solução deve permitir automatizar a remoção ou suspensão de Usuários-Administradores, Usuários-Aprovadores e Usuários-Alvo (colaboradores) de férias ou que saíram da empresa, através da API.

8. SEGURANÇA DE ACESSO E APLICAÇÃO

8.1. A solução deve suportar múltiplos fatores de autenticação no seu acesso para usuários-administradores, no mínimo 03 (três) opções, incluindo uso de credenciais, *tokens* e localidades confiáveis.

8.2. A solução deve suportar habilitar quaisquer níveis de segurança individualmente, de acordo com a política de segurança.

8.3. A solução deve controlar o perfil de acesso de cada usuário individualmente, permitindo somente as atividades permitidas através de perfis de acesso, tais como somente leitura, edição de modelos, edição de campanhas, painéis e acesso completo.

8.4. A solução deve controlar usuários através de times com funções específicas em níveis de aprovação de modelos e campanhas.

8.5. A solução não deve limitar a quantidade de times e aprovações, e cada modelo só poderá ser usado após ser aprovado, e cada campanha só será enviada após sua respectiva aprovação.

8.6. A solução deve segmentar todos os acessos e dados dos usuários da CMB através de portal exclusivo, acessível através de endereços com o nome da organização.

8.7. A solução deve suportar autenticação segura integrada com soluções da *Microsoft Teams* (*Office* 365).

8.8. A solução deve permitir o cadastramento de domínios confiáveis para interação dos usuários com a plataforma.

8.9. A solução deve permitir o cadastramento de etiquetas customizáveis (logotipo) para organização, filtros e relatórios de acordo com a estrutura organizacional.

8.10. A solução deve suportar a restrição de acesso para usuários-administradores através da utilização de redes ou localidades confiáveis.

9. PORTAL PESSOAL DOS USUÁRIOS-ALVO

9.1. A solução deve possuir um ambiente virtual portal pessoal individual para cada usuário-alvo (colaborador) que permita realizar quaisquer treinamentos enviados, visualizar quaisquer mensagens enviadas e ter acesso a conteúdo adicional, como: *ebooks* e cartilhas adicionais ao tema de segurança digital, a serem criados pela CMB.

9.2. A solução deve permitir que apenas o próprio usuário-alvo tenha acesso *online* ao seu ambiente virtual individual.

9.3. A solução deve permitir o envio de lembretes periódicos por *e-mail* e ilimitados para os usuários-alvo acessarem seus ambientes virtuais individuais.

9.4. A solução não deve contabilizar financeiramente o uso de lembretes para os ambientes virtuais individuais, podendo a CMB utilizar destes lembretes ilimitados durante toda a vigência deste CONTRATO.

10. CRIPTOGRAFIA DE DADOS

10.1. A solução deve obter 100% de pontuação no "**Teste *TOP* – *Site***" do serviço https://top.nic.br.

10.2. A solução deve adotar controles de segurança entre eles, criptografia para manter a segurança de qualquer informação da CMB em seu ambiente.

10.3. A solução deve segmentar os dados em container, com controles de segurança adicionais, que permitem fazer *backup* e restaurar dados individuais conforme necessário.

11. INTEGRAÇÃO DA SOLUÇÃO, INTEGRAÇÃO DOS DADOS E API

11.1. A solução deve permitir a utilização através de todos os serviços e clientes de *e-mail*, bem como, navegadores utilizados pela CMB.

11.2. A solução deve permitir a integração dos resultados com plataformas de SIEM.

11.3. A solução deve permitir a integração dos resultados em formato CSV, XLSX e JSON.

11.4. A solução deve permitir filtrar online quais grupos serão exportados, como campanhas, domínios, etiquetas e tipos das mensagens.

11.5. A solução deve permitir a exportação dos resultados em arquivos compactados ou sem compactação.

11.6. A solução deve permitir o fornecimento dos dados em *log* bruto (inalterado em sua geração original).

11.7. A solução deve permitir o fornecimento dos dados em horário *global* UTC.

11.8. A solução deve permitir o fornecimento dos dados completos, sem nenhum tipo de filtro, a qualquer momento através do portal *web*, relatórios, *backup* de banco de dados e API.

11.9. A solução deve disponibilizar API própria para obter em tempo real acesso a todos dados disponíveis.

11.10. A solução deve disponibilizar documentação pública da API contendo todos os *endpoints* e exemplos para rápida integração.

11.11. A API da solução deve permitir integração com os sistemas de dados internos, como o SIEM.

11.12. A solução deve permitir auditoria completa de todos os acessos, objetos e mudanças na plataforma.

11.13. A auditoria da solução deve ser disponível através da plataforma *online*, relatórios e API.

11.14. A API da solução deve permitir automatizar e manipular Listas de Contatos e Contatos através dos sistemas internos ou comandos diretos.

11.15. A API da solução deve permitir automatizar e manipular Usuários através dos sistemas internos ou comandos diretos.

11.16. A API da solução deve permitir gestão completa de Usuários, Listas de Contatos, Contatos e Dados.

12. ARQUITETURA TECNOLÓGICA DA SOLUÇÃO

12.1. A solução deverá ser disponibilizada em arquitetura SaaS (*Software as a Service*), sem a necessidade de implantação ou disponibilidade de servidores locais pela contratada.

12.2. A solução deve ser hospedada em provedor *SaaS* que possua, no mínimo, certificação SOC tipo II.

12.3. A solução deve suportar o auto escalonamento de processamento sem custo adicional para a CMB.

12.4. A solução deve suportar a recuperação de desastres (*desaster recovery*).

12.5. A solução deve rodar em alta disponibilidade dos serviços.

12.6. A solução deve suportar o escalonamento sazonal de processamento para picos de consumo, incluindo os períodos de grande utilização das soluções a serem integradas.

12.7. A solução não deve depender de *hardware* físico homologado em ambiente computacional da CMB.

12.8. A solução não deve depender de *software* homologado em ambiente computacional da CMB.

12.9. A solução deve permitir integração nativa com os canais de comunicação: do *Microsoft Office* 365 (*Outlook e Microsoft Teams*)

12.10. As informações da CMB devem ser mantidas em território nacional, bem como respeitar todas as legislações vigentes quanto ao tratamento e privacidade dos dados.

12.11. O conteúdo das mensagens e treinamentos devem ser entregues por uma *Content Delivery Network (*CDN ou Rede de Fornecimento de Conteúdo) que possua 2 ou mais pontos de acesso no Brasil.

13. CRONOGRAMA DE EXECUÇÂO DA SOLUÇÂO

13.1. Cronograma estimado:

Etapas	Descrição	Prazos
1	Assinatura do contrato com a definição do início da vigência	n/a
2	Reunião inicial de *kick off*	Até 02 (dois) dias úteis
3	Configurações iniciais e testes	Até 10 (dez) dias úteis
4	Treinamentos e orientações. *Hands-on*	Até 10 (dez) dias úteis
5	Execução completa da solução e entrega a CMB	Até 20 (vinte) dias úteis
6	Aceite técnico da solução	Até 02 (dois) dias úteis
7	Solução em produção	Até 02 (dois) dias úteis

14. GERENCIAMENTO DE CICLO DE VIDA DE DADOS

14.1. A solução deve confirmar e excluir os dados de forma iterativa das camadas de seus aplicativos e armazenamento.

14.2. A CONTRATADA deve possuir processos contra destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso aos dados da CMB.

14.3. A CONTRATADA deve remover todos os dados da CMB após término de contrato.

ETAPAS:

PRAZO DE VIGENCIA DA CONTRATAÇÃO: O prazo de vigência da contratação é de 12 (doze meses), ou seja 1 (um ano), contados da assinatura do instrumento contratual, podendo ser prorrogado por iguais e sucessivos períodos ou frações, até o limite de 60 (sessenta) meses.

LOCAL DE EXECUÇÃO DO SERVIÇO: Plataforma *Online* (Modalidade *SAAS*).

PRAZO DE INÍCIO E CONCLUSÃO: Previsão de início no exercício de 2024 e conclusão no ano exercício de 2025 caso o serviço não seja renovado. E em até 7 dias úteis após a assinatura do contrato e após o treinamento na plataforma a contratada deverá disponibilizar a solução para consumo.

PRAZO DE RECEBIMENTO DEFINITIVO (Aceite/Atesto): 20 dias consecutivos.

REGIME DE EXECUÇÃO DOS SERVIÇOS: Os serviços serão executados por preço unitário.

PRAZO DE PAGAMENTO: Até 30 (trinta) dias após a apresentação da Nota Fiscal.

ACORDO DE NÍVEL DE SERVIÇOS: Níveis Mínimos de Serviço.

- Níveis de serviço são critérios objetivos e mensuráveis estabelecidos entre CONTRATANTE e CONTRATADA com a finalidade de aferir e avaliar fatores relacionados à solução contratada, principalmente qualidade, desempenho e disponibilidade.
- A CONTRATADA deverá cumprir os prazos para atendimento e solução dos chamados, conforme critérios definidos na Tabela - Níveis de Serviço.
- Ao solicitar o serviço, será informado o indicador de nível de criticidade para mensurar os fatores das situações-problema.

Tabela - Níveis de Serviço

NÍVEL	PRAZO PARA ATENDIMENTO (HORAS CORRIDAS)	PRAZO PARA SOLUÇÃO (HORAS CORRIDAS)
Crítica	Em até 2 horas, em regime de 24x7x365	Em até 4 horas, após abertura de chamado, em regime de 24x7x365
Alta	Em até 2 horas, em regime de 8x7x365	Em até 6 horas, após abertura de chamado, em regime de 8x7x365
Média	Em até 2 horas, em regime de 8x7x365	Em até 8 horas, após abertura de chamado, em regime de 8x7x365
Baixa	Em até 2 horas, em regime de 8x5x365	Em até 12 horas, após abertura de chamado, em regime de 8x5x365

- A solução do problema implica no retorno à condição normal de funcionamento de todos os serviços impactados. O prazo de resolução é contado a partir da abertura do chamado pela CONTRATANTE.
- A Tabela Situações típicas para acionamento de Suporte Técnico combina os diferentes graus de interrupção dos serviços com algumas situações típicas para atendimento de chamados de suporte técnico.

- São definidos os seguintes graus de interrupção dos serviços:

  - ✓ **A**: serviço totalmente interrompido em um ou mais pontos de acesso;
  - ✓ **B**: serviço parcialmente interrompido;
  - ✓ **C**: defeito não causa interrupção do serviço, apenas degrada sua qualidade.

Tabela - Situações típicas para acionamento de Suporte Técnico

Situação	Grau de interrupção	Nível de Criticidade
Falha no Sistema	A	Crítica
	B	Alta
	C	Baixa
Base de dados do Sistema	A	Crítica
	B	Alta
	C	Baixa
Falha no disparo de uma simulação de ataque	A	Alta
	B	Média
	C	Baixa
Falha na automatização de grupos e subgrupos	A	Alta
	B	Baixa
	C	Baixa
Falha na disponibilização de conteúdos	A	Crítica
	B	Alta
	C	Média
Falha no Fluxo de Aprovações	A	Alta
	B	Média
	C	Baixa

- Decorrido os prazos previstos na Tabela Níveis de Serviço, sem o atendimento devido, fica a CONTRATANTE autorizada a aplicar medidas corretivas, sanções e penalidades à CONTRATADA dentro dos parâmetros explicitados neste Termo de Referência, respeitado o direito a apresentação de justificativas cabíveis para posterior avaliação, por parte do Fiscal do Contrato designado pela CONTRATANTE;
- Qualquer que seja o problema apresentado na prestação do serviço, a CONTRATADA deverá arcar com todos os custos e procedimentos necessários à sua solução, incluindo a substituição de qualquer equipamento, se for necessário;
- A CONTRATADA deverá encaminhar ao fiscal técnico do contrato, até o 5º (quinto) dia útil após o atendimento, o Relatório de visita contendo, pelo menos, as seguintes informações:

- ✓ Data e hora da abertura do chamado;
- ✓ Nome do solicitante;
- ✓ Data e hora do início do atendimento;
- ✓ Data e hora da resolução do problema;
- ✓ Descrição do problema, incidente ou solicitação atendida e Procedimentos efetuados.

- Caso sejam apurados resultados abaixo do Nível de Serviço acordado, é garantido à CONTRATADA o direito de apresentar justificativas cabíveis para posterior avaliação, por parte do Fiscal do Contrato designado pela CONTRATANTE;
- As justificativas, devidamente fundamentadas, aceitas pelo Gestor e pelo Fiscal do Contrato poderão anular a incidência de glosas e advertências na aplicação do Nível de Serviço Mínimo.

Tabela - Glosas

SEVERIDADE	ATENDIMENTO	AÇÕES
CRÍTICA	Após decorrido o prazo para atendimento do chamado e/ou do prazo para solução do problema. (Indicado na Tabela Níveis de Serviço)	Glosa de até 1% (um por cento) sobre o valor da Nota Fiscal, por hora excedente, sem prejuízo de eventuais sanções administrativas, a critério da CONTRATANTE. Caso o somatório das glosas aplicadas ultrapasse 8% (oito por cento) do valor total do contrato, poderá ensejar a rescisão do Contrato, independentemente da aplicação de sanções cabíveis.
ALTA	Após decorrido o prazo para atendimento do chamado e/ou do prazo para solução do problema. (Indicado na Tabela Níveis de Serviço)	Glosa de até 0,8% (oito décimos por cento) sobre o valor da Nota Fiscal, por hora excedente, sem prejuízo de eventuais sanções administrativas, a critério da CONTRATANTE. Caso o somatório das glosas aplicadas ultrapasse 12% (doze por cento) do valor total do contrato, poderá ensejar a rescisão do Contrato, independentemente da aplicação de sanções cabíveis.
MÉDIA	Após decorrido o prazo para atendimento do chamado e/ou do prazo para solução do problema. (Indicado na Tabela Níveis de Serviço)	Glosa de até 0,5% (cinco décimos por cento) sobre o valor da Nota Fiscal, por hora excedente, sem prejuízo de eventuais sanções administrativas, a critério da CONTRATANTE. Caso o somatório das glosas aplicadas ultrapasse 20% (vinte por cento) do valor total do contrato, poderá ensejar a rescisão do Contrato, independentemente da aplicação de sanções cabíveis.

BAIXA	Após decorrido o prazo para atendimento do chamado e/ou do prazo para solução do problema. (Indicado na Tabela Níveis de Serviço)	Glosa de até 0,2% (dois décimos por cento) sobre o valor da Nota Fiscal, por hora excedente, sem prejuízo de eventuais sanções administrativas, a critério da CONTRATANTE. Caso o somatório das glosas aplicadas ultrapasse 20% (vinte por cento) do valor total do contrato, poderá ensejar a rescisão do Contrato, independentemente da aplicação de sanções cabíveis.

Tabela - Indicadores mensais individuais: IIS

Indicador	**Índice de Indisponibilidade da Solução - IIS**
Processo	Plataforma de Segurança
Periodicidade da Avaliação	Mensal
Definição	Mede o percentual de indisponibilidade dos serviços prestados
Forma da Avaliação	Pelo fiscal do contrato, através de ferramentas que permitam a avaliação dessa disponibilidade
Fórmula de Cálculo	IIS = Somatório dos tempos em que a Solução está indisponível / Tempo (em horas) referente a 1 (um) mês x 100%
Considerações gerais	O percentual da glosa será aplicado sobre o valor do serviço de *Data Center*
Meta	99% de disponibilidade
Glosas	Para 1% < IIS ≤ 1,25%; glosa de 0,3% Para 1,25% < IIS ≤ 1,50%; glosa de 0,5% Para 1,50% < IIS ≤ 1,75%; glosa de 1,0% Para IIS > 1,75%; glosa de 2,0%

ANEXO II

PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS

Item	Descrição do Serviço/Custo	Composição	Quantidade	Valor Total (12 meses)
01	Serviço de plataforma *SAAS*, para simulação de ataque de *Phishing* e treinamento direcionado aos usuários da rede corporativa da CMB.	- Plataforma *SAAS* - Simulador de *phishing* - Biblioteca de conteúdos de cibersegurança e conformidade - Campanhas e disparos ilimitados por *e-mail* - Comunicações automatizadas de todas as fases - Treinamentos, questionários, aceite *online* e políticas - *Dashboards* dos indicadores, relatórios *online,* integrações com APIs e exportação de dados - Autenticação em múltiplos fatores (MFA) - Integração Segura para Acesso e Dados (*Microsoft*) - Automatização de campanhas e treinamentos por classificação (*ranking*) - Agendamento de campanhas - Controle de acesso para conteúdo de campanhas - Suporte *Online* 24x7 - Plataforma de *gamification* e conhecimento pessoal - Vídeos com *tags* personalizadas - API para automação e gerenciamento de dados - Perfis e grupos de aprovação - Retenção de *logs* em aderência a leis de privacidade, proteção de dados e auditoria - Integração com a plataforma de comunicação *Teams* e *Outlook* - *Smishing* e comunicados de acordo com o número de usuários - Domínios personalizados - *Benchmarking* com a Indústria	1	R$
VALOR GLOBAL PARA 12 MESES				

ANEXO III

CRONOGRAMA FÍSICO-FINANCEIRO

Item	Descrição do Serviço	Prazo	% do Valor Contratado
01	Configuração inicial das contas administrativas da equipe da CMB e demais configurações da solução.	5 dias	0%
02	Configuração da integração com *Azure Active Directory* (*Azure AD*) e *ADFS* (se for o caso).	5 dias	0%
03	Treinamento completo aos usuários-administradores (*hands-on) de* todas as funcionalidades da solução disponibilizadas a CMB.	10 dias	0%
04	Conclusão de uma execução completa de uma campanha. (simulação de *phishing*, treinamento, gamificação, informes de *e-mails* e *dashboards* e relatórios e demais ações necessárias de testes).	20 dias	0%
05	Serviço entregue e disponível para a CMB consumir	2 dias	50%
06	Solução em produção na CMB	Mensal	50% (dividido em 11x)

ANEXO IV

CONSULTA PÚBLICA CMB Nº ##/20##

IDENTIFICAÇÃO DA PROPONENTE

Razão Social: _____

Telefone: _____

E-mail de contato: _____

CONTRIBUIÇÕES E SUGESTÕES: