ESTUDO TÉCNICO PRELIMINAR (ETP)

Em conformidade com a **Resolução n.º 468/2022-CNJ**
Guia de Contratações de STIC do Poder Judiciário

Processo Administrativo n.º 33826/2023

Contratação de empresa especializada na prestação de serviços continuados, sem dedicação exclusiva de mão de obra, para subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos online, na modalidade de Ensino à Distância (EaD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais.

São Luís (MA), julho de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor(es)
01/07/2024	1.0	Finalização da primeira versão do ETP.	Jairo Ferreira …
17/07/2024	1.1	Revisão do ETP.	Carlos José L… Ricardo Luis C… Marcos Aurelio… José Eduardo … hallyson.nasci…
21/07/2024	1.2	Revisão final do ETP.	Jairo Ferreira …

ESTUDO TÉCNICO PRELIMINAR (ETP)

1. INTRODUÇÃO

O Estudo Técnico Preliminar (ETP) tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Processo n.º 33826/2023, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

A segurança da informação é crucial para proteger os dados e a integridade das operações do TJMA, garantindo a confidencialidade, a integridade e a disponibilidade das informações judiciais.

Distorções cognitivas são frequentemente combinadas com subterfúgios técnicos na engenharia social como método de ataque para comprometer sistemas organizacionais, visando ganhos financeiros (ProofPoint).

O phishing é um dos principais vetores de ataques cibernéticos e foi o mais utilizado nos últimos anos, segundo o Federal Bureau of Investigation (FBI), com mais de 255 milhões de registros em 2022, o que representa um aumento de 61% em relação a 2021, segundo a SlashNext, resultando em mais de 91% dos vazamentos de dados, conforme reportado pela KnowBe4.

Devido ao aumento dos ataques cibernéticos reportados pelo CERT.br e por outras instituições, o TJMA intensificou seus investimentos em ações de segurança da informação.

Considerando a quantidade de caixas de correio eletrônico que o TJMA possui, principal meio de comunicação institucional e vetor frequente de ataques, é essencial conscientizar cada usuário de e-mail.

Incidentes de segurança da informação podem comprometer a confiança do público no sistema judicial e causar danos irreparáveis às partes envolvidas. Portanto, é fundamental que todos estejam cientes e preparados para lidar com tais situações.

Os usuários do TJMA precisam estar capacitados para identificar, prevenir e responder a ameaças de segurança cibernética, essencial para proteger sistemas e dados institucionais.

O uso de tecnologias de informação no ambiente judicial exige alto nível de conhecimento e práticas adequadas de segurança da informação e proteção de dados pessoais. Iniciativas de educação, treinamento e conscientização de usuários devem ser personalizadas e adaptadas às necessidades individuais de servidores, magistrados e estagiários.

A capacitação contínua e atualizada em segurança da informação e proteção de dados pessoais é essencial para garantir a eficácia das medidas de segurança e acompanhar a evolução das ameaças cibernéticas.

A implementação de programas de treinamento e capacitação contribui para o estabelecimento de uma cultura de segurança institucional, alinhando todos os integrantes do TJMA às melhores práticas de segurança de mercado.

Como cada usuário de e-mail do TJMA é um potencial foco de ataque cibernético, as iniciativas de treinamento e conscientização devem ser eficientes e atender às necessidades individuais dos servidores.

Qualquer abordagem de Segurança da Informação que não considere os usuários como um ponto vulnerável aumenta significativamente o risco de incidentes que podem causar vazamentos de dados sigilosos, comprometimento da integridade de dados e indisponibilidade de serviços. Portanto, é crucial utilizar soluções que possam:

- Identificar usuários que necessitam de treinamento em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, através de campanhas de phishing do TJMA;

- Mapear o perfil dos usuários em relação às boas práticas de segurança na utilização do e-mail corporativo;

- Gerar estatísticas de uso para identificar elementos que possam confundir o usuário a clicar em links maliciosos ou responder a e-mails de phishing;

- Consolidar os dados coletados para permitir a análise crítica e a avaliação de ações pela Alta Administração, mitigando riscos relacionados à utilização do e-mail corporativo; e

- Proporcionar ferramentas e recursos educacionais para capacitar os usuários conforme suas necessidades individuais.

Portanto, justifica-se a necessidade de contratar uma solução integrada para campanhas de phishing e treinamento, capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais.

2.1 Identificação das Necessidades de Negócio (NN)

ID	NECESSIDADES DE NEGÓCIO (NN)
NN1	Subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos online, na modalidade de Ensino à Distância (EaD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, pelo período de 36 meses.
NN2	Suporte técnico especializado para a plataforma integrada de campanhas de phishing e treinamentos online.
NN3	Treinamento para administração da plataforma integrada de campanhas de phishing e treinamentos online.

2.2 Identificação das Necessidades Tecnológicas (NT)

ID	NECESSIDADES TECNOLÓGICAS (NT)	Alinhamento às Necessidades de Negócio
NT1	Disponibilidade de ativo de TIC (computador ou notebook) ou de dispositivo móvel (tablet ou smartphone) contendo navegador web, a exemplo do chrome, firefox, ou microsoft edge.	NN1, NN2 e NN3
NT2	Disponibilidade de acesso à Internet.	NN1, NN2 e NN3

3. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO COM PCA/PCTIC 2024

A contratação está alinhada ao objetivo estratégico do Poder Judiciário do Estado do Maranhão (PJMA) de reestruturar a Tecnologia da Informação (Governança, Serviços e Infraestrutura), ao objetivo do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) de promover a capacitação na área de Tecnologia da Informação para magistrados e servidores (M.13) e ao Plano de Contratações de Tecnologia da Informação e Comunicação (PCTIC), disponível em https://www.tjma.jus.br/atos/portal/geral/506635/128/pnao.

Reestruturar a Tecnologia da Informação (Governança, Serviços e Infraestrutura)

ALINHAMENTO AO PCA/PCTIC 2024 - Link Planilha PCTIC 2024:	
Código	**Descrição do objeto**
24DE00088	Serviço de treinamento na área de Segurança da Informação para usuários(as) de TIC

4. REQUISITOS DA CONTRATAÇÃO

4.1 Requisitos necessários e suficientes à escolha da Solução de TIC.

NN1: Subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos online, na modalidade de Ensino à Distância (EaD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, pelo período de 36 meses.

Gerais:

ID	Requisitos
R1.01	Suportar o idioma português do Brasil (pt-br).
R1.02	Disponibilizar documentação de uso da plataforma, incluídos na própria plataforma ou não, no idioma português do Brasil (pt-br).
R1.03	Disponibilizar relatórios gerenciais dos usuários e campanhas de phishing.
R1.04	Possibilitar emissão de certificado de participação de cada curso que o usuário concluir, contendo pelo menos o nome completo do participante, título do curso, conteúdo abordado e carga horária.
R1.05	Estar disponível 24 horas por dia, 7 dias por semana (24x7), exceto nas situações de manutenção previstas.
R1.06	Ser acessível para pessoas com deficiência, em conformidade com padrão WCAG (versão 2 ou superior).*

Técnicos:

ID	Requisitos
R1.07	Ser totalmente provida em nuvem para sua plena execução, sem a necessidade de servidor adicional, IP dedicado para disparos de e-mail, registro de domínios, aquisição de equipamento ou módulos extras, etc.
R1.08	Suportar o protocolo HTTPs.
R1.09	Suportar recurso multifator de autenticação (MFA). Caso não tenha suporte nativo, deve permitir a integração com solução de MFA de terceiros ou realizar a autenticação via Single Sign-On (SSO).**
R1.10	Possibilitar a importação facilitada e em lote de contas do Active Directory (AD), Lightweight Directory Access Protocol (LDAP) ou SAMBA.
R1.11	Disponibilizar API para exportação das informações incluídas na plataforma (usuários, campanhas de phishing, simulados, etc.).
R1.12	Possuir interface gráfica web para os perfis de administrador e usuário, no idioma português do Brasil (pt-br).
R1.13	A interface gráfica web deve ser compatível, minimamente, com os principais navegadores de Internet do mercado.
R1.14	As licenças da plataforma devem ser atribuídas de forma não permanente aos usuários, permitindo que, ao desativar ou excluir um usuário, a licença seja liberada para nova utilização.
R1.15	Ser entregue configurada e pronta para uso.

Phishing:

ID	Requisitos
R1.16	Possibilitar a criação e administração ilimitadas de campanhas de phishing.
R1.17	Possuir informações gerenciais das campanhas de phishing.
R1.18	Possuir templates prontos e customizáveis para serem utilizados em campanhas de phishing.
R1.19	Possuir estrutura própria de envio de e-mails (serviço de SMTP) para disparar os e-mails de simulação de phishing.
R1.20	Não deve haver limites para a quantidade de disparos de mensagens de e-mail das campanhas de phishing.
R1.21	Não deve haver restrição de quantidade de templates que podem ser criados ou utilizados na plataforma.

Conteúdos, Materiais e Avaliações:

ID	Requisitos
R1.22	Oferecer conteúdos e materiais na área de Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, este último aplicado à legislação brasileira.
R1.23	Os conteúdos audiovisuais, como vídeos e podcasts, bem como os materiais escritos, como textos e apostilas, devem ser disponibilizados no idioma português do Brasil (pt-br).
R1.24	Os conteúdos audiovisuais, como vídeos e podcasts podem ter legendas de forma complementar no idioma português do Brasil (pt-br).
R1.25	Permitir a criação de trilhas de treinamentos personalizados.
R1.26	Disponibilizar formas de avaliação para validar o aprendizado dos conteúdos, utilizando questionários, testes, jogos e quizzes, todos no idioma português do Brasil (pt-br).
R1.27	Permitir a inclusão de materiais da contratante, como arquivos digitais em formato PDF.
R1.28	Disponibilizar atualizações dos conteúdos dos cursos e materiais conforme a evolução da plataforma integrada de campanhas de phishing e treinamentos online.

NN2: Suporte técnico especializado para a plataforma integrada de campanhas de phishing e treinamentos online.

ID	Requisitos
R2.01	Prestar suporte técnico de segunda a sexta-feira, durante o horário comercial.

NN3: Treinamento para administração da plataforma integrada de campanhas de phishing e treinamentos online.

ID	Requisitos

R3.01	Capacitar os administradores do ambiente nos principais recursos da plataforma, no modo presencial ou EAD síncrono (online e ao vivo).
R3.02	Disponibilizar materiais para facilitar a administração da plataforma, como vídeos, gravações, tutoriais, e outros materiais considerados importantes.
R3.03	Realizar treinamento da equipe da contratante que administrará a solução, com duração mínima de 20 (vinte) e máxima de 40 (quarenta) horas.

*** R1.06 – Ser acessível para pessoas com deficiência, em conformidade com padrão WCAG (versão 2 ou superior).**

Trata-se de exigência com objetivo de não excluir os usuários do TJMA que possuem deficiência visual, auditiva ou motora. É necessário que a solução contratada atenda a esse público, de modo que não sejam preteridos em relação aos servidores sem deficiência. A produção de conteúdo nesses padrões mostra que a plataforma está preocupada com a inclusão digital. A exigência atende à Resolução n.º 401, de 16 de junho de 2021, do Conselho Nacional de Justiça (CNJ), em especial o artigo 2º que diz: “A fim de promover a igualdade, devem ser adotadas, com urgência, medidas apropriadas para eliminar e prevenir quaisquer barreiras urbanísticas ou arquitetônicas, de mobiliários, de acesso aos transportes, nas comunicações e na informação, atitudinais ou tecnológicas.”

**** R1.09 – Suportar recurso multifator de autenticação (MFA). Caso não tenha suporte nativo, deve permitir a integração com solução de MFA de terceiros ou realizar a autenticação via Single Sign-On (SSO).**

A exigência está alinhada com a Portaria n.º 140, de 22 de abril de 2024, do Conselho Nacional de Justiça (CNJ), que determina a implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis. Apesar da plataforma em questão não ser classificada como um sistema judicial sensível, o duplo fator de autenticação é essencial como um segundo nível de proteção, além do login e senha, para assegurar que usuários e administradores tenham acesso seguro aos dados.

Por exemplo, uma violação da plataforma que comprometa apenas o login e senha poderia expor informações críticas, como:

- Identificação dos usuários menos treinados no TJMA;

- Usuários que mais falharam em testes de engenharia social e campanhas de phishing;

- Informações pessoais, como nome, e-mail e outras disponíveis na plataforma.

Com essas informações, um invasor poderia direcionar ataques específicos e ter sucesso ao tentar invadir a instituição. Portanto, é crucial que essa exigência de segurança seja mantida pela Administração.

4.2 Realizar avaliação das necessidades de adequação do ambiente do Tribunal:

Não se aplica tendo em vista se tratar de solução tecnológica que não será implantada na infraestrutura tecnológica da contratante.

5. ESTIMATIVA DAS QUANTIDADES PARA A CONTRATAÇÃO

A quantidade de licenças para acesso à plataforma integrada de campanhas de phishing e treinamentos online é estimada em 7.000 (sete mil), considerando o número de usuários (magistrados, servidores e estagiários) de todas as unidades administrativas e judiciais do Tribunal de Justiça do Estado do Maranhão (TJMA).

O quantitativo é baseado no número de caixas de correio eletrônico de usuários ativos no ambiente do Google Workspace, excluindo as das unidades administrativas e judiciais. O número de usuários ativos no Active Directory (AD) também foi considerado para validação da análise.

Foi considerada a quantidade de estagiários ativos e o ingresso de novos servidores no TJMA por meio do concurso público em andamento.

Além das 7.000 licenças, é esperada a contratação de 540 (quinhentas e quarenta) horas de suporte técnico para configuração, atualização e manutenção da plataforma integrada de campanhas de phishing e treinamentos online, e 5 (cinco) vagas de treinamento para administradores e transferência de conhecimento para uso da plataforma.

6. LEVANTAMENTO DE MERCADO

6.1 Identificação das soluções

ID	Descrição da solução
1	HSC MindAware
2	KnowBe4 Security Awareness Training
3	KASPERSKY AUTOMATED SECURITY WARENESS PLATFORM
4	PROOFPOINT

Da análise das possíveis soluções de mercado, constatou-se que apenas o item 4 não foi pesquisado ou precificado, pois sua plataforma não atende ao requisito R1.12 disposto no subitem 4.1, estando disponível apenas no idioma inglês.

6.2 Solução similar existente no "Portal do Software Público Brasileiro" - http://www.softwarepublico.gov.br

Não há solução deste tipo que atenda os requisitos funcionais e técnicos.

6.3 Software livre

Não há solução deste tipo que atenda os requisitos funcionais e técnicos.

6.4 Contratos de órgão ou entidade pública

Foram identificadas contratações de objetos similares por outros órgãos da Administração Pública. Entretanto, não foram encontradas Atas de Registro de Preço vigentes que atendessem à demanda disposta no subitem 2.1 (NN1, NN2 e NN3).

As contratações da Administração Pública apresentam especificidades distintas uma da outra de acordo com as necessidades de cada órgão contratante.

6.4.1 Para as pesquisas realizadas com órgãos ou entidades públicas, registram-se o que segue:

a) Cotação A:

O contrato n.º 5841/00, decorrente do Pregão Eletrônico n.º 22/2023, Tipo Menor Preço, celebrado entre o órgão PROCERGS - CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO GRANDE DO SUL S.A., CNPJ n.º 87.124.582/0001-04 e a empresa QUALITEK TECNOLOGIA LTDA., CNPJ n.º 10.224.281/0001-10, conforme detalhamento abaixo:

Item	Descrição	Unidade	Qnt	Valor
1	Fornecimento de licenças de uso de plataforma integrada de campanhas de phishing e treinamentos online, especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação, pelo período de 24 meses, de acordo com o subitem 2.3.1, cláusula 2ª do presente instrumento contratual.	licença	1001	R$ 6.500,00
2	Serviço gerenciado especializado incluindo suporte técnico e atualizações, configuração, treinamento e transferência de conhecimento, pelo período de 24 meses, de acordo com o subitem 2.3.2, cláusula 2ª do presente instrumento contratual.	meses	24	R$ 900,00
			MENSAL	R$ 7.400,00

O valor de R$ 6.500,00 (mensal) dividido pela quantidade de 1001 licenças resultou no valor unitário de **R$ 6,49** para o item 1**.**

Consta no subitem 3.2.16 do Contrato que “A empresa a ser contratada deverá disponibilizar serviço de suporte técnico e manutenção, no regime 8x5 (oito horas por dia, cinco dias por semana) pelo período de 24 (vinte e quatro) meses.”

O suporte técnico 8x5 é baseado no valor de **R$ 900,00** por mês para o item 2, incluindo o treinamento na sua composição.

b) Cotação B:

O Tribunal de Justiça do Estado de Pernambuco (TJPE), CNPJ n.º 11.431.327/0001-34, por meio do Pregão Eletrônico, tipo Menor Preço, n.º 154/2023 - NLCD, celebrou o contrato n.º 14/2024-TJPE com a empresa QUALITEK TECNOLOGIA LTDA., CNPJ n.º 10.224.281/0001-10, conforme detalhamento abaixo:

Item	Descrição	Unidade	Qnt	Valor
1	Assinatura (Subscription) para Ferramenta de Phishing Educativo KNOWBE4, na versão Diamond, para 8 mil contas de e-mail por 3 anos.	UND	1	R$ 643.000,00
2	Suporte técnico especializado	HORAS	600	R$ 30.000,00
			VALOR	R$ 673.000,00

O valor de R$ 643.000,00 dividido por 36 meses, resultou em R$ 17.861,11 por mês. Dividido pela quantidade de 8000 licenças, resultou no valor unitário de **R$ 2,23** para o item 1**.**

O valor de R$ 30.000,00 dividido pela quantidade de horas contratada (600h), resultou no valor de **R$ 50,00** para o item 2.

6.5 Proposta comercial de mercado

Com base nos requisitos funcionais, especialmente nos estruturantes de negócio, foram pesquisadas no mercado plataformas integradas de campanhas de phishing e capacitação em segurança da informação que atendessem às necessidades identificadas. Foram buscadas soluções que:

a) fossem amplamente reconhecidas no campo da conscientização em segurança da informação;

b) oferecessem a maior biblioteca de conscientização e capacitação na língua portuguesa;

c) incluíssem treinamento prático por meio de simulações de phishing, técnica de engenharia social mais utilizada por invasores;

d) fornecessem indicadores de evolução da maturidade dos usuários e da instituição durante a execução do programa;

e) permitissem gestão integrada de todos os recursos.

Assim, orçamentos foram solicitados por e-mail para empresas que pudessem atender à solução demandada. Vale destacar que algumas dessas empresas não responderam à pesquisa de preço por falta de interesse ou por a solução ofertada não atender aos requisitos especificados.

6.5.1 Para as solicitações de proposta comercial de mercado por e-mail, registram-se o que segue:

a) Cotação C - ANEXO A:

A pesquisa de preço realizada com a empresa HSC DESENVOLVIMENTO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA, CNPJ n.º 13.103.980/0001-08 trouxe o seguinte valor:

Part Number	Descrição	Unidade	Qnt	Valor
LMD360-1K	HSC MindAware - Licença de uso HSC MindAware 360º + Suporte técnico - 36 meses	licença	8000	R$ 68,20
MD360-TRAINING	Treinamento on-line e transferência de conhecimento carga horária 12 horas para até 5 pessoas.	serviço	5	R$ 2.500,00

O valor da licença de R$ 68,20, originado do somatório dos itens Licença de Uso e Suporte Técnico com Part Number LMD360-1K, dividido pela quantidade de 12 meses resultou no valor unitário de **R$ 5,68**.

O valor unitário do treinamento com Part Number MD360-TRAINING, considerando uma carga horária de 12 horas, foi definido em **R$ 2.500,00** por aluno.

b) Cotação D - ANEXO B:

A pesquisa de preço realizada com a empresa ALUS IT SECURITY, CNPJ n.º 26.748.686/0001-97 trouxe o seguinte valor:

Item	Descrição	Unidade	Qnt	Valor
1	KnowBe4 Security Awareness Training Subscription Diamond +5000 users 3 year	licença	7000	R$ 235,00
2	AST85S - ALUS - Suporte Técnico 8x5 Soluções	horas	540	R$ 300,00
3	Treinamento Knowbe4 40 horas	unidade	1	R$ 12.000,00

O valor de R$ 235,00 dividido por 3 anos resultou em R$ 78,33 por ano. Este valor, dividido por 12 meses, resultou no valor unitário de **R$ 6,52** para o item 1**.**

O suporte técnico 8x5 é baseado em 15 horas por mês, com um valor de **R$ 300,00** por hora para o item 2.

O treinamento para 2 turmas de 10 alunos, considerando cada turma com 40 horas, totaliza **R$ 1.200,00** por aluno para o item 3.

c) Cotação E - ANEXO C:

A pesquisa de preço realizada com a empresa NETWORK SECURE SEGURANÇA DA INFORMÁTICA LTDA, CNPJ n.º 05.250.796/0001-54 trouxe o seguinte valor:

Item	Descrição	Unidade	Qnt	Valor
1	KASPERSKY AUTOMATED SECURITY WARENESS PLATFORM (KASAP) 36 MESES - 5000+ users	licença	7000	R$ 1.334.410,00
2	Suporte remoto 10 horas/mês - Período 36 meses	horas	360	R$ 120.000,00
3	A implantação será feita junto com o Treinamento Hands'on, repassando o conhecimento para o cliente. Implantação	unidade	1	R$ 50.000,00

	da ferramenta e criação de 1 campanha.			

O valor de R$ 1.334.410,00 dividido por 36 meses, resultou em R$ 37.066,94 por mês. Dividido pela quantidade de 7000 licenças, resultou no valor unitário de **R$ 5,29** para o item 1**.**

O valor de R$ 120.000,00 dividido por 360 horas, resultou no valor de **R$ 333,00** por mês para o item 2.

O valor do item 3 não será utilizado, pois foi considerado inexequível.

7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Primeiramente, cumpre sublinhar que os valores apresentados a seguir constituem mera estimativa.

A tabela abaixo resume os valores estimados para contratação:

NN***	COTAÇÃO					Preço Médio
	A	B	C	D	E	
NN1	R$ 6,49	R$ 2,23	R$ 5,68	R$ 6,52	R$ 5,29	R$ 5,24
NN2	R$ 900,00	R$ 50,00	-	R$ 300,00	R$ 333,33	R$ 395,83
NN3	-	-	R$ 2.500,00	R$ 1.200,00	-	R$ 1.850,00

***** NN - Necessidades de Negócio - definidas no subitem 2.1 ***

A cotação ¨A¨ não inclui o item NN3 separadamente. Já a cotação ¨B¨ não possui o item NN3. Na cotação ¨E¨ o item NN3 não será utilizado, pois foi considerado inexequível.

As tabelas abaixo resumem os valores estimados e o quantitativos para contratação:

NN1: Subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos online, na modalidade de Ensino à Distância (EaD), voltados à capacitação

e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, pelo período de 36 meses.

NN	UND	Preço Médio	Valor			
	Licenças		1º ano (12 meses)	2º ano (12 meses)	3º ano (12 meses)	Total (36 meses)
NN1	7000	R$ 5,24	R$ 440.160,00	R$ 440.160,00	R$ 440.160,00	R$ 1.320.480,00

NN2: Suporte técnico especializado para a plataforma integrada de campanhas de phishing e treinamentos online.

NN	UND	Preço Médio	TOTAL
	Horas		
NN2	540	R$ 395,83	R$ 213.748,20

NN3: Treinamento para administração da plataforma integrada de campanhas de phishing e treinamentos online.

NN	UND	Preço Médio	TOTAL
	Unidades		
NN3	5	R$ 1.850,00	R$ 9.250,00

RESUMO:

DESCRIÇÃO	Valor			
	1º ano	2º ano	3º ano	Total
NN1: Subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos online, na modalidade de Ensino à Distância (EaD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, pelo período de 36 meses.	R$ 440.160,00	R$ 440.160,00	R$ 440.160,00	R$ 1.320.480,00

NN2: Suporte técnico especializado para a plataforma integrada de campanhas de phishing e treinamentos online.	R$ 213.748,20	-	-	R$ 213.748,20
NN3: Treinamento para administração da plataforma integrada de campanhas de phishing e treinamentos online.	R$ 9.250,00	-	-	R$ 9.250,00
	R$ 663.158,20	**R$ 440.160,00**	**R$ 440.160,00**	**R$ 1.543.478,20**

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

Contratação de empresa especializada na prestação de serviços continuados, sem dedicação exclusiva de mão de obra, para subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos online, na modalidade de Ensino À Distância (EAD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, para atender à demanda do Poder Judiciário do Estado do Maranhão, conforme requisitos definidos no subitem 4.1.

9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Com o objetivo de otimizar a competitividade e garantir economia de escala, os itens técnicos especializados deste ETP devem ser agrupados para serem fornecidos por uma única empresa, conforme o §3º do art. 40 da Lei n.º 14.133/2021. Esta medida visa reduzir custos de gestão contratual e/ou promover maior vantagem na contratação dos serviços.

As Necessidades do Negócio (NN) NN1 e NN2, detalhadas no subitem 2.1**,** serão pagas anualmente, enquanto a necessidade NN3 será paga após a execução do treinamento aos administradores da plataforma, conforme resumo abaixo:

NN	PERÍODO	PAGAMENTO / ENTREGA
NN1	1º Ano	Pagamento da 1ª Parcela - equivalente a 12 meses de uso das licenças da plataforma.

NN1	2º Ano	Pagamento da 2ª Parcela - equivalente a 12 meses de uso das licenças da plataforma.
NN1	3º Ano	Pagamento da 3ª Parcela - equivalente a 12 meses de uso das licenças da plataforma.
NN2	Mensal	Pagamento mensal - equivalente a quantidade de horas efetivamente utilizadas, num total de 540 horas.
NN3	-	Pagamento a ser emitido após a execução do treinamento - equivalente à conclusão do treinamento para administração da plataforma integrada de campanhas de phishing e treinamentos online.

10. DEMONSTRATIVAS DOS RESULTADOS PRETENDIDOS

A aquisição da plataforma integrada de campanhas de phishing e treinamentos online poderá trazer os seguintes benefícios:

#	Benefícios a serem alcançados com a contratação
01	Aumento da conscientização sobre as melhores práticas de segurança da informação.
02	Melhoria na compreensão dos riscos e ameaças cibernéticas.
03	Fortalecimento das habilidades em identificar e reportar incidentes de segurança.
04	Redução do número de incidentes de segurança causados por erros humanos.
05	Aumento da adesão às políticas e diretrizes de segurança da informação.
06	Melhoria na proteção dos dados e informações sensíveis do PJMA.
07	Criação de uma cultura de segurança da informação, tornando-se agentes ativos na proteção dos recursos digitais do Judiciário.
08	Maior confiança e satisfação em relação à segurança das informações e sistemas do PJMA.

11. PROVIDÊNCIAS A SEREM ADOTADAS PREVIAMENTE A CELEBRAÇÃO DO CONTRATO

Para a execução dos serviços de contratação da plataforma integrada de campanhas de phishing e treinamentos online haverá necessidade das adequações abaixo:

- Exportar dados dos usuários do Active Directory (AD) ou do Gmail para alimentar a plataforma integrada de campanhas de phishing e treinamentos online;

- Ajustar o ambiente do Google Workspace, especificamente o aplicativo do Gmail, para garantir que as campanhas de phishing cheguem corretamente às caixas de correio dos usuários;

- Realizar testes de acessos de administrador e de usuário na plataforma;

- Conduzir testes de campanhas de phishing para um grupo de usuários.

12. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

O Contrato PJMA n.º 22/2022 (Processo n.º 15709/2021) contém o número de licenças em uso no serviço de e-mail do Google Workspace (GW), facilitando o cálculo do total de licenças a serem adquiridas para a plataforma integrada de campanhas de phishing e treinamentos online. O cálculo não considerou as licenças de e-mail usadas pelas unidades administrativas e judiciais do TJMA no ambiente do GW.

É importante sinalizar que existe uma correlação indireta entre as contratações devido às campanhas de phishing da plataforma integrada de campanhas de phishing e treinamentos online que serão encaminhadas para as caixas de correio eletrônico dos usuários. No entanto, não há interdependência entre o objeto do Contrato PJMA n.º 22/2022 e o objeto da contratação pretendida, pois uma não depende da outra para funcionar ou estar disponível.

Ante o exposto, não foram identificadas outras contratações do TJMA a serem observadas para fins de registro de correlação ou interdependência.

13. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS

Não foram encontrados critérios de sustentabilidade incidentes sobre o objeto a ser licitado/contratado.

14. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO

Os Estudos Técnicos Preliminares evidenciaram que a solução escolhida consiste na contratação de empresa especializada na prestação de serviços continuados, sem dedicação exclusiva de mão de obra, para subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos online, na modalidade de Ensino à Distância (EaD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, com valor global estimado de **R$ 1.543.478,20** (um milhão, quinhentos e quarenta e três mil, quatrocentos e setenta e oito reais e vinte centavos).

A aquisição da solução tecnológica proposta permitirá alcançar o resultado desejado, ou seja, atender à necessidade identificada neste ETP ao estabelecer uma abordagem preventiva contra riscos cibernéticos por meio da conscientização dos usuários internos sobre os serviços e infraestrutura tecnológica do TJMA de maneira construtiva e pedagógica.

Nesse contexto, destaca-se que atualmente o TJMA não possui meios e ferramentas para avaliação comportamental de usuários, nem para automatização das ações necessárias de conscientização decorrentes dessa avaliação. Especificamente, falta a capacidade de utilizar recursos pedagógicos para conscientização dos usuários de Tecnologia da Informação e Comunicação (TIC).

Verifica-se, portanto, a necessidade crucial de adquirir uma solução tecnológica de conscientização para mitigar os riscos institucionais relacionados à Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais.

Vale ressaltar que anteriormente a este Estudo Técnico Preliminar (ETP), ainda na fase de elaboração do Documento de Oficialização de Demanda (DOD) sem o devido conhecimento do objeto a ser adquirido, o mesmo denominava-se de “Contratação de serviço de conteúdo para treinamento e conscientização dos(as) usuários(as) de TIC do Poder Judiciário do Estado do Maranhão (PJMA), por meio de acesso à plataforma online (modalidade EAD), especializada na oferta de conteúdos de capacitação e conscientização em Segurança da Informação.”

Após a conclusão do ETP, o objeto foi refinado e passou a ser denominado **"Contratação de empresa especializada na prestação de serviços continuados, sem dedicação exclusiva de mão de obra, para subscrição de licença de plataforma integrada de campanhas de phishing e treinamentos online, na modalidade de Ensino à Distância (EaD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais"**.

15. APROVAÇÃO E ASSINATURAS

A Equipe de Planejamento da Contratação foi instituída pelo ATO DA PRESIDÊNCIA-GP n.º 109, de 24 de julho de 2024.

INTEGRANTE TÉCNICO	INTEGRANTE DEMANDANTE
ASSINADO DIGITALMENTE JAIRO FERREIRA ROCHA A conformidade com a assinatura pode ser verificada em: http://serpro.gov.br/assinador-digital SERPRO **Integrante Técnico** Jairo Ferreira Rocha 138404	CLAUDIO HENRIQUE CARNEIRO SAMPAIO:42774918391 Assinado de forma digital por CLAUDIO HENRIQUE CARNEIRO SAMPAIO:42774918391 DN: c=BR, o=ICP-Brasil, ou=AC SOLUTI Multipla v5, ou=35622406000190, ou=Presencial, ou=Certificado PF A3, cn=CLAUDIO HENRIQUE CARNEIRO SAMPAIO:42774918391 Dados: 2024.08.30 17:10:45 -03'00' **Integrante Demandante** Cláudio Henrique Carneiro Sampaio 99176

AUTORIDADE MÁXIMA DA ÁREA DE TIC
CLAUDIO HENRIQUE CARNEIRO SAMPAIO:42774918391 Assinado de forma digital por CLAUDIO HENRIQUE CARNEIRO SAMPAIO:42774918391 DN: c=BR, o=ICP-Brasil, ou=AC SOLUTI Multipla v5, ou=35622406000190, ou=Presencial, ou=Certificado PF A3, cn=CLAUDIO HENRIQUE CARNEIRO SAMPAIO:42774918391 Dados: 2024.08.30 17:10:56 -03'00' Cláudio Henrique Carneiro Sampaio Diretor de Tecnologia da Informação e Comunicação 99176