TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS
Avenida André Araújo, nº 200 - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tre-am.jus.br

ESTUDO TÉCNICO PRELIMINAR - ETP Nº 0000107838 - TRE-AM/PRES/SETRIB /STI/COINF

1. OBJETO

Contratação de licenças de acesso a plataforma integrada de treinamento online, na modalidade "Software as Service" (SaaS), especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação.

1.1.Natureza do objeto

O objeto da contratação possui natureza comum, nos termos do parágrafo único, do art. 1º, da Lei nº 10.520/2002, c/c art. 4º do Decreto nº 10.024/2019.

1.2.Classificação do objeto

Classifica-se o objeto da contratação como bens ou serviços de informática, nos termos do Decreto nº 7.174/2010.

2. NECESSIDADE DA CONTRATAÇÃO

2.1.Motivação

As pessoas são o elo mais fraco quando falamos em segurança cibernética. Costumam ser a porta de entrada para que criminosos cibernéticos invadam a rede e roubem informações valiosas, causando grandes prejuízos financeiros e de imagem às instituições, notadamente aos órgãos públicos. Assim, treinar e conscientizar pessoas é primordial para o fortalecimento da segurança da infraestrutura tecnológica e dos dados pessoais.

Diante disso, o Conselho Nacional de Justiça (CNJ), por meio da Portaria nº 162/2021, aprovou, entre outros, o Anexo VII – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário (PECSC-PJ). Trata-se de um Manual de Referência que tem por finalidade, entre outras, desenvolver e fortalecer a cultura, a educação, a conscientização e as habilidades em segurança cibernética dos usuários de TIC e de Segurança da Informação, alcançando magistrados, servidores, estagiários, terceirizados e colaboradores em geral.

Nessa senda, o Tribunal Superior Eleitoral (TSE) previu a contratação de solução para conscientização em segurança da informação na Estratégia Nacional de Cibersegurança da Justiça Eleitoral (processo SEI 0005695-28.2021.6.08.8000), "Anexo I - Arquitetura de Cibersegurança, item SG10 - PID10 – Solução para Conscientização SI". A estratégia prevê que os servidores e colaboradores devem ser capacitados a fim de reduzir os riscos na área de segurança cibernética. É importante que os funcionários entendam os objetivos da segurança da informação e o impacto potencial, positivo e negativo, do seu próprio comportamento na organização.

Além disso, a contratação pretendida supre recomendação formulada pelo Tribunal de Contas da União (TCU) no Acórdão 3143/2021 - SEI 0678959, inicialmente direcionada ao TSE, para implementação de um programa permanente de orientação e treinamento em segurança da informação para servidores, estagiários, colaboradores e voluntários:

> ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, diante das razões expostas pelo Relator,
>
> 9.1. recomendar, com fulcro no art. 250, III, do RI/TCU, c/c o art. 11, da Resolução TCU 315/2020, ao Tribunal Superior Eleitoral que:
>
> (...)
>
> 9.1.5. implemente um programa permanente de orientação e treinamento em segurança da informação para servidores, colaboradores, estagiários e voluntários, à semelhança das orientações do item 7.2.2 da NBR ISO/IEC 27002:2013 e do Controle 14 do CIS, v.8, em cumprimento ao inciso VI do art. 15 do Decreto 9.367/2018 c/c o inciso III do art. 11 da Resolução TSE 23.644/2021;

Apesar de direcionada ao TSE, a recomendação precisa ser aplicada em toda a Justiça Eleitoral, visto que a infraestrutura tecnológica é totalmente conectada e a falta de conhecimento de um usuário, em qualquer um dos Regionais, pode implicar em uma invasão que comprometerá toda a rede.

2.2.Fundamentação legal

- Decreto nº 9.637/2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
- Resolução TSE nº 23.644/2021: Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
- Resolução CNJ nº 370/2021: Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CNJ nº 396/2021: Institui a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ);
- Instrução Normativa SGD-ME nº 1/2019: Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

3. RESULTADOS ESPERADOS

Com a presente contratação, espera-se um crescimento acentuado da maturidade dos usuários de TIC do TRE-AM com relação à segurança da informação.

4. ALINHAMENTO AO PDTI E AO PEI

A presente contratação encontra-se alinhada ao Plano Estratégico Institucional (PEI) do TRE-AM, notadamente quanto ao Objetivo Estratégico “Fortalecer a estratégia nacional de TIC e de proteção de dados”. Encontra-se alinhada, ainda, ao Plano Diretor de TIC (PDTIC), notadamente quanto ao vetor “Pessoas”, Iniciativa IN-12-17 – Capacitar a equipe técnica e usuários acerca da importância da segurança da informação no âmbito do TRE/AM.

5. REQUISITOS FUNCIONAIS DA CONTRATAÇÃO

5.1.Requisitos de negócio

A fim de tornar-se um dos pilares para a execução de um programa permanente de conscientização em segurança da informação no âmbito do TRE-AM, a solução deve prover, no mínimo, os seguintes recursos:

5.1.1. Disponibilizar ampla biblioteca de conteúdos de segurança da informação, inclusive LGPD, em língua portuguesa.
5.1.2. Entregar conhecimento com uso de recursos interativos, como vídeo, simulações, quizzes (questionários rápidos), boletins informativos, etc.
5.1.3. Possibilitar a inclusão de cursos produzidos pela própria Justiça Eleitoral ou por terceiros, gerenciando-os juntamente com os conteúdos nativos da solução.
5.1.4. Permitir a execução de campanhas e simulações de treinamento automatizadas, em especial, simulações de phishing (mensagens eletrônicas que são armadilhas para roubar dados e inserir vírus na rede).
5.1.5. Permitir o carregamento de políticas e normas de segurança da Justiça Eleitoral como conteúdo, a fim de que os usuários estudem (leiam) e efetuem o aceite.
5.1.6. Permitir acompanhamento da evolução da maturidade dos usuários e da instituição em relação à Segurança da Informação.
5.1.7. Permitir a gestão completa de treinamento e usuários.
5.1.8. Permitir integração com a base de dados de usuários da instituição.
5.1.9. Para essa contratação é premissa que a plataforma permita automatização de tarefas, tendo em vista a necessidade de racionalização de recursos humanos. Atribuição automática de treinamentos, agendamento de campanhas de phishing e apoio técnico na execução do programa de conscientização através da plataforma são fatores fundamentais para o atingimento dos objetivos propostos.

5.2.Requisitos de capacitação, ambientais, culturais e sociais

5.2.1. Deve haver uma instrução no modelo hands-on para os gestores da plataforma.
5.2.2. Deve possuir conteúdo acessível à deficientes auditivos e visuais.
5.2.3. Permitir a inclusão da identidade visual da instituição nas campanhas e treinamentos.
5.2.4. Ambiente da plataforma deve ser disponibilizado totalmente em português

5.3.Requisitos de manutenção e garantia

5.3.1. Durante todo o período de contrato deve haver profissional especializado apto a prestar suporte aos gestores da plataforma no esclarecimento de dúvidas, acessível no período de 8 (oito) horas por dia, 5 (cinco) dias da semana, dias úteis.
5.3.2. A contratada deve garantir o quantitativo mínimo de treinamentos estabelecido neste Estudo Técnico.

5.4.Requisitos Temporais

5.4.1. O mercado, em geral, oferece licenças de acesso pelo período de 1 (um) ano a 3 (três) anos. Tendo em vista a necessidade de o Poder Judiciário estabelecer um programa permanente de conscientização, conforme preconiza a Portaria CNJ nº 162/2021, há necessidade de um contrato

que permita a longo prazo avaliar a evolução da maturidade em segurança da informação. Assim, o prazo de vigência das licenças deve ser o máximo possível, que, neste caso, são 3 (três) anos.

5.4.2. A plataforma de treinamento deve estar disponível no período de 24h x 7d para os usuários, durante toda a vigência da contratação.

5.5. Requisitos de Segurança da Informação

5.5.1. Deve ser assinado termo de sigilo e confidencialidade para garantir a segurança física e lógica de todos os documentos, cópias e informações digitais, onde a contratada se compromete a manter sigilo de quaisquer informações de ambiente tecnológico e de negócio da contratante a que tiver acesso durante a realização deste serviço. O termo de sigilo e confidencialidade deve conter, ainda, cláusulas específicas que obriguem e estabeleçam prazos para que a contratada, após o término do contrato, elimine todo e qualquer dado pessoal da contratante na plataforma.

5.5.2. Garantir a segurança das informações dos usuários carregadas na plataforma.

5.5.3. Garantir que as informações produzidas no decorrer do programa não sejam perdidas por interrupção ou término do contrato.

Em relação aos dados pessoais controlados pela CONTRATANTE, esclarecemos que não haverá, no âmbito do CONTRATO, o compartilhamento de dados pessoais ou dados pessoais sensíveis com a CONTRATADA.

6. REQUISITOS TÉCNICOS DA CONTRATAÇÃO

6.1.Características Gerais

6.1.1. Acesso ilimitado à biblioteca com, no mínimo, 300 (trezentos) itens de conteúdo de segurança da informação em português ou em língua estrangeira com legendas em português. Requisitos adicionais:

6.1.1.1. Plataforma deve estar em conformidade com o padrão WCAG (versão 2 ou superior), para atender as necessidades de usuários com deficiências visuais, auditivas, motoras e cognitivas

6.1.1.2. Deve haver conteúdo específico voltado a LGPD Brasileira.

6.1.2. Entregar conhecimento através de conteúdos tais como: vídeos, games, quizzes, artes (posteres), assessments (avaliações).

6.1.3. Prover gerenciamento de usuários e cursos, permitindo:

6.1.3.1. Seleção de módulos de treinamento para grupo de usuários;

6.1.3.2. Atribuição automática de treinamentos para novos usuários;

6.1.3.3. Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes;

6.1.3.4. Carga de usuários por meio de arquivo .CSV;

6.1.3.5. Integração com o AD (Active Directory) da contratante;

6.1.3.6. Inativação de usuários sem perda do histórico de dados;

6.1.3.7. Permitir que uma licença de acesso utilizada por um usuário desligado da contratante possa ser aplicada a um novo usuário, durante o período remanescente do contrato. Neste caso, não é necessária a manutenção do histórico do usuário
antigo.

6.1.4. Permitir inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários.

6.1.5. Permitir a carga de conteúdos próprios de treinamento em segurança da Informação da contratante, em vídeo, no formato PDF ou no padrão SCORM.

6.1.5.1. Todas as funcionalidades de gestão disponíveis para os conteúdos nativos devem poder ser aplicadas aos conteúdos próprios da contratante.

6.1.6. Permitir a carga e o aceite de políticas e normas de segurança da informação da contratante.
6.1.7. Prover ambiente de gestão para acompanhamento online de progressão e desempenho dos usuários.
6.1.8. Disponibilizar detalhes sobre a porcentagem de inscrições, cursos iniciados, incompletos, concluídos e conhecimento da política de segurança e normas.
6.1.9. Prover ambiente de gestão que possibilite a criação de grupos de usuários com base em comportamento frente às simulações e treinamentos realizados.
6.1.10. Disponibilizar relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos.
6.1.11. Permitir a emissão de certificados para os treinamentos.
6.1.12. Prover APIs de relatórios que permitam personalizar os documentos, integrando-os a outros sistemas de negócios para apresentar os dados a partir da plataforma.
6.1.13. Disponibilizar perfis de acesso para gestão de campanhas e treinamentos (desejável também perfil para auditoria, porém não obrigatório).
6.1.14. Possibilitar a autenticação em dois fatores para usuários e administradores.
6.1.15. Possibilitar a criação de campanhas simuladas de phishing, a fim de avaliar o comportamento dos usuários;
6.1.15.1. Permitir criação de número ilimitado de campanhas durante a vigência do contrato;
6.1.15.2. Disponibilizar pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos diretamente pela contratante;
6.1.15.3. Manter histórico por usuário e por campanha;
6.1.15.4. Permitir que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação.
6.1.16. Possibilitar a criação automatizada de um programa personalizado em segurança da informação ou fazer a recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários.
6.1.17. Apresentar painel gerencial com indicador de nível de risco em segurança da informação para cada usuário e para a instituição. O nível de risco deve ser medido considerando-se pelo menos dois fatores: participação em treinamentos e avaliação
nos testes de phishing.
6.1.18. Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br).
6.1.19. Para evitar dependência tecnológica, a plataforma deve prover APIs que permitam a exportação contínua de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante. Informações como evolução da maturidade dos usuários (nível de risco), cursos efetuados, certificados, resultados de testes de phishing, etc, devem ser passíveis de exportação através de APIs. Essa característica permite que a Justiça Eleitoral, ao término do contrato, possa
prosseguir com seu programa contínuo de capacitação, na forma determinada pelo TCU no Acórdão Plenário 3143/2021.

6.2. Implantação e suporte

6.2.1. A contratada deve disponibilizar, durante todo período contratual, um gerente de contas para apoiar e orientar a contratante no uso da plataforma. O gerente de conta tem como atribuições:
6.2.1.1. Acompanhar o projeto (programa de conscientização);
6.2.1.2. Esclarecer dúvidas;
6.2.1.3. Sugerir proativamente novos caminhos para o programa;
6.2.1.4. Ser ponte com o suporte técnico;
6.2.1.5. Configurar a conta e fazer a integração com a infraestrutura da contratante (*onboarding*).
6.2.2. As atividades do gerente de contas podem ser desenvolvidas remotamente, com uso de meios de

comunicação digital.

6.2.3. A contratada deve efetuar, a partir das informações fornecidas pela contratante, a implantação da solução (*onboarding*), tarefa que consiste na configuração e integração da infraestrutura tecnológica da contratante com a plataforma. A tarefa
envolve, sempre que aplicável, no mínimo:

6.2.3.1. Inclusão das informações dos servidores da contratada em listas de permissão (*whitelisting*) da contratante;

6.2.3.2. Configuração da integração com Active Directory e ADFS;

6.2.3.3. Carregamento dos usuários (extraídos do AD) e classificação em grupos;

6.2.3.4. Habilitação de Duplo Fator de Autenticação.

6.2.4. Deve ser agendada no mínimo 1 (uma) reunião por videoconferência entre o gerente de contas e os administradores da contratante para passagem de conhecimento, durante o período de onboarding.

6.2.4.1. A passagem de conhecimento deve envolver, no mínimo:

- Melhores práticas para implantação;
- Forma de Acesso dos usuários e download de conteúdos;
- Criação de grupos inteligentes;
- Atribuição de treinamentos a grupos de usuários;
- Carga de conteúdos da contratante;
- Criação e automatização de campanhas de phishing;
- Criação de roles (papeis) de segurança;
- Carga, inativação e exclusão de usuários;
- Personalização de identidade visual; Emissão e extração de relatórios;

6.2.4.2. Toda instrução e passagem de conhecimento é aberta ao quantitativo de profissionais necessários para gestão da plataforma, a critério da contratante.

6.2.4.3. A contratante poderá ainda, a seu critério, solicitar a inclusão de qualquer outro tema relacionado às especificações constantes neste termo de referência.

6.2.5. A critério da contratante, podem ser solicitadas outras reuniões por videoconferência com o gerente de contas durante a vigência do contrato.

6.3. Qualificação Técnica e financeira

6.3.1. Apresentar atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove ter a licitante executado, satisfatoriamente, o fornecimento de no mínimo 1000 (mil) licenças de acesso à plataforma de conscientização ofertada.

6.3.1.1. Será aceito o somatório de atestados de períodos concomitantes para certificar que todo o quantitativo indicado na cláusula anterior já tenha sido fornecido pela licitante.

6.3.2. Apresentar, para fins de qualificação econômico-financeira, certidão negativa de feitos sobre falência, recuperação judicial ou recuperação extrajudicial, expedida pelo distribuidor da sede da licitante, que se encontre dentro do prazo de validade. Caso não haja prazo de validade especificado no documento, será considerado o prazo máximo de 30 (trinta) dias, contados da data de sua expedição.

6.4. Vigência e prazos

6.4.1. A tabela abaixo descreve o cronograma executivo e a vigência da contratação:

ETAPA	DESCRIÇÃO	PRAZO
1	**Assinatura do Contrato**	**Dia D**

2	Reunião – Alinhamento do programa e apresentação de funcionalidades da plataforma	D+5
3	**Entrega da fase 1 – Liberação das licenças de acesso à plataforma**	**D+5 (E1)**
4	Apresentação do documento fiscal – Fase 1	D+7
5	Aceite Técnico Definitivo – Fase 1	D+9
6	Pagamento – Fase 1 (60% do total)	D+19
7	**Entrega da Fase 2 – Configurar a conta, fazer carga de usuários e a integração com a infra da contratante (*onboarding*)/ Repasse de conhecimento**	**D+30 (E2)**
8	Apresentação do documento fiscal – Fase 2	D+35
9	Aceite técnico definitivo – Fase 2	D+37
10	Pagamento – Fase 2 (40% do total)	D+47
11	Vigência das licenças de acesso	(E1)+36 meses

Tabela 1: Cronograma executivo

6.4.2. Todos os prazos serão contados em dias úteis. Havendo antecipação das entregas, os prazos posteriores serão automaticamente antecipados.

6.5. Análise da dependência tecnológica

6.5.1. Em termos gerais, busca-se contratar uma plataforma com conteúdo de conscientização e treinamento para a Justiça Eleitoral. Quanto a esse aspecto não há que se falar em dependência tecnológica. Funciona como qualquer outra plataforma de treinamento: os cursos ficam disponíveis somente durante a vigência contratual, Neste período podem ser iniciados e finalizados, sem qualquer restrição. Após o término do contrato o acesso ao conteúdo não é mais permitido.

6.5.2. No entanto, há que se considerar outros aspectos relacionados aos requisitos de negócio estabelecidos, que não implicam em uma dependência tecnológica propriamente dita, mas indicam a necessidade de alguns cuidados no que tange à gestão no término do contrato. São eles:

a) Certificados de conclusão dos Cursos;
b) Avaliação de maturidade em segurança dos usuários e da instituição;
c) Conteúdos da contratante disponibilizados na plataforma;
d) Aceite das normas de segurança da informação.

6.5.3. Antes do término do contrato, a contratante deverá efetuar a exportação de todo o conteúdo, tais como: certificados, relatórios de nível de risco, cursos próprios inserido na plataforma e relação das normas com os respectivos aceites e providenciar uma nova forma de armazenamento e gestão, ou com recursos tecnológicos próprios ou através de novos contratos.

6.5.4. Está sendo exigido que a plataforma possua APIs internas que permitam que essa exportação seja feita ao longo do contrato. Os Tribunais podem trabalhar em conjunto para utilizar essas APIs de forma que a solução final de exportação seja padronizada e útil da toda a Justiça Eleitoral.

7. AVALIAÇÃO DAS SOLUÇÕES DE MERCADO

A. Solução similar que possa ser disponibilizada por outro órgão ou entidade da Administração Pública

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

B. Solução similar existente no "Portal do Software Público Brasileiro" – http://www.softwarepublico.gov.br – (aplicável somente para o caso de Solução de Tecnologia da Informação e Comunicação que envolva software)

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

C. Software livre ou software público

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

D. Solução de mercado, comercial.

Com base nos requisitos funcionais, em especial os requisitos de negócio estruturantes, buscou-se no mercado plataformas de capacitação em segurança da informação que fossem aderentes às necessidades. Assim, buscou-se empresas/soluções que:

1. Fossem notoriamente reconhecidas nesse campo de atuação - conscientização em segurança da informação.
2. Disponibilizassem a maior biblioteca de conscientização e capacitação em português (em linguagem nativa ou legendado).
3. Agregassem o recurso prático de treinamento dos usuários através de simulações de phishing, que é, hoje, a técnica de engenharia social mais usada por invasores contra os usuários de tecnologia da informação.
4. Permitissem a integração de conteúdo da Justiça Eleitoral, a exemplo de treinamentos de capacitação já produzidos por alguns Regionais, como Minas Gerais e Rio Grande do Norte, o que permite a construção de um ambiente único de treinamento, facilitando os esforços de gestão.
5. Trouxessem o indicador de evolução da maturidade dos usuários e da instituição durante a execução do programa.
6. Disponibilizassem a gestão integrada de todos os recursos.

Foram analisadas as plataformas **Hackers Rangers**, **KnowBe4** e **Proofpoint**, a partir das especificações técnicas constantes neste ETP. A tabela abaixo apresenta o resultado da análise:

Avaliação de plataformas para programa permanente de conscientização em segurança da informação					
Tema	**Característica**	**Item do ETP**	**Hackers Rangers**	**KnowBe4**	**ProofPoint**
Conteúdo nativo	Conteúdo em língua portuguesa ou legendado em português nacional (300 itens)	6.1.1.	Não (80)	Sim (486)	Sim (403)
	Conteúdo LGPD Nacional	6.1.1.2.	Sim	Sim	Sim
	Entregar conhecimento através de conteúdos tais como: vídeos, games, quizzes, artes (posteres), assessments (avaliações).	6.1.2.	Sim	Sim	Sim

	Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior)	6.1.1.1.	N/A	Sim	Sim
Conteúdo do cliente	Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (Moodle, usado pela JE)?	6.1.5.	Parcial/ Não permite SCORM	Sim	Não
	Todas as funcionalidades da plataforma aplicáveis ao conteúdo nativo são aplicáveis ao conteúdo da contratante inserido na plataforma?	6.1.5.1.	Sim	Sim	Não
Implantação e segurança	Possui integração com AD?	6.1.3.5.	Sim	Sim	Sim
	Carga de usuários por meio de arquivos .csv?	6.1.3.4.	Sim	Sim	Sim
	Permite duplo fator de autenticação para usuários e administradores?	6.1.14.	Não	Sim	Não
Normas de segurança como conteúdo	Permite a inclusão dos normativos de segurança da contratante e o aceite pelos usuários? Formato .pdf	6.1.5. e 6.1.6.	Não	Sim	Não
Automação	Atribuição automática de treinamento para novos usuários?	6.1.3.2.	Não, a plataforma tem como base a gamificação	Sim	Sim
	Criação automatizada de um programa personalizado em segurança da informação ou recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários?	6.1.16.	Não	Sim	Não
	APIs que permitam a exportação de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante para guarda ou integração com outros sistemas?	6.1.12. e 6.1.19.	Não	Sim	Sim

Gestão de usuários e cursos	Seleção de módulos de treinamento para grupo de usuários? (Atribuição de treinamentos).	6.1.3.1.	Não	Sim	Sim
	Gestão de cursos, tais como: porcentagem de inscrições, cursos iniciados, incompletos, concluídos	6.1.8.	Sim	Sim	Sim
	Acompanhamento online de progressão e desempenho dos usuários?	6.1.7.	Sim	Sim	Sim
	Emissão de Certificados para os cursos?	6.11.	Não	Sim	Sim
	Relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos?	6.1.10.	Sim	Sim	Sim
	Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes?	6.1.3.3.	Não, o adm envia e-mails	Sim	Sim
	Inativação de usuários sem perda do histórico de dados?	6.1.3.6.	-	Sim	Sim
	Disponibilizar perfis de acesso para gestão de campanhas e de treinamentos?	6.1.13.	Sim	Sim	Sim
	Provê ambiente de gestão que possibilita a criação de grupos de usuários com base em comportamento frente às simulações e treinamentos realizados?	6.1.9.	Sim	Sim	Sim
	Possibilita a atribuição da licença de acesso de um usuário que foi desligado da instituição para um novo usuário (neste caso não é necessário manter o histórico)?	6.1.3.7.	Sim	Sim	Sim
Campanhas de phishing	Permite a criação de número ilimitado de campanhas durante a vigência do contrato?	6.1.15.1.	Sim	Sim	Sim
	Disponibiliza pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos	6.1.15.2.	Sim	Sim	Sim

	pela contratante?				
	Mantem histórico por usuário e por campanha?	6.1.15.3.	Sim	Sim	Sim
	Permite que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação?	6.1.15.4.	Sim	Sim	Sim
Indicador de maturidade em segurança	Possui indicador de nível de risco em segurança da informação para cada usuário e para a instituição? O nível de risco deve ser medido considerando-se pelo menos dois fatores: participação em treinamentos e avaliação nos testes de phishing.	6.1.17.	Não	Sim	Não
Suporte técnico	A contratada disponibiliza durante todo período contratual um gerente de contas para apoiar e orientar a contratante no uso da plataforma, com as atribuições previstas no item 6.2.1?	6.2.1. 6.2.2. 6.2.4.	Sim	Sim	Sim
	Repasse de conhecimento	6.2.3.	Sim	Sim	Sim
Customização	Permite inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários?	6.1.4.	Sim	Sim	Sim
Linguagem da plataforma	Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br)	6.1.18.	Sim	Sim	Não

Entre as plataformas analisas, a Knowbe4 foi a única que atendeu integralmente aos requisitos propostos. Assim, é fundamental que seja devidamente demonstrada a legítima necessidade da Administração em relação às exigências que conduziram a este resultado:

1) Item 6.1.1.1. Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior)

Trata-se de exigência com objetivo de não excluir os servidores, estagiários e colaboradores da Justiça Eleitoral 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 inclusão digital. A exigência atende à resolução CNJ 401/2021, em especial o artigo 2º, quando cita a eliminação de barreiras tecnológicas: *A fim de*

promover a igualdade, deverão 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.

2) Item 6.1.14. Possibilitar a autenticação em dois fatores para usuários e administradores.

O duplo fator de autenticação é um mecanismo de segurança que cria um 2º nível de segurança, além do login e senha, para que os usuários e administradores tenham acesso aos dados na plataforma. No caso dessa contratação, uma invasão através do comprometimento do login e senha poderia dar acesso a informações valiosíssimas para um invasor. Ele teria acesso a, por exemplo:

a) Quais os usuários menos treinados na Justiça Eleitoral;
b) Quais usuários mais falharam nos testes de engenharia social;
c) Informações pessoais como nome, CPF, e-mail e outras disponíveis na plataforma.
    a. De posse dessas informações, o invasor poderia direcionar os ataques de engenharia social para esses usuários e ter sucesso em uma invasão à instituição.
    b. Assim, é imprescindível que essa exigência voltada à segurança seja mantida pela Administração.

3) Item 6.1.17. Indicador de Maturidade em Segurança da Informação.

O Acórdão TCU Plenário 3143/2021 recomenda a implantação de um programa permanente de conscientização. É fundamental que a solução proporcione uma forma efetiva de avaliar a evolução da maturidade do Órgão em segurança, visando a definição dos caminhos a serem seguidos na condução do programa. Neste contexto, o indicador de evolução de maturidade é primordial. Os parâmetros mínimos para este indicador são relativamente simples e estão claramente descritos – treinamentos realizados e avaliação dos testes de phishing. Cabe acrescentar que a tarefa de efetuar cálculos manuais de maturidade a partir de informações de centenas usuários não é razoável. Conforme já abordado neste Estudo, há necessidade de racionalizar a força de trabalho do TRE-AM, que já é muito reduzida, voltando o esforço do corpo de servidores para tarefas fins que não são passíveis de automação.

4) Item 6.1.19. APIs para exportação dos dados.

A própria redação do item já traz a justificativa de sua necessidade. A funcionalidade tem como objetivo evitar dependência tecnológica. A resolução CNJ nº 182/2013, em seu art. 18, §3, III, "a", 8, determina que o termo de referência deve prever mecanismos para minimizar a dependência técnica da contratada. As APIs permitem a exportação contínua de todas as informações gerenciais da plataforma de conscientização para a base de dados da própria contratante, tais como o nível de risco
dos usuários, cursos efetuados, certificados, resultados de testes de phishing, etc.

5) Itens de automação 3.3.2- Atribuição automática de treinamentos para novos usuários e 3.16 - Possibilitar a criação automatizada de um programa personalizado em segurança da informação ou fazer a recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários.

Os itens de automação alinham-se com a necessidade de racionalização da força de trabalho da justiça eleitoral, além de estabelecer padrões claros para o treinamento dos usuários, especialmente para aqueles que acabaram de ingressar no Órgão, sem qualquer conhecimento da cultura e do contexto de segurança da

informação em seu novo ambiente de trabalho. A atribuição automática de um conjunto de treinamentos para os novos usuários permite um nivelamento mínimo inicial que fortalecerá a segurança da informação do órgão. A criação automática de programas personalizados com base no indicador de maturidade justifica-se pelos mesmos motivos: racionalização de recursos humanos e padronização do programa.

E. Escolha da solução

O Estudo teve por base a comparação de três das principais soluções, onde apenas a plataforma KnowBe4 mostrou atender integralmente os requisitos desejados. Contudo, esta equipe de planejamento da contratação entende que, diante da dinâmica do mercado, há possibilidade de existirem outras plataformas que não foram analisadas.

Assim, não obstante a Knowbe4 ser supostamente a única plataforma que atende integralmente as exigências, o Termo de Referência não trará indicação de marca, apresentando somente as necessidades da Administração. Isso permitirá que todos os players do mercado possam trazer questionamentos que julgarem pertinentes a respeito de qualquer uma das especificações constantes no Termo.

Importante considerar que a Administração Pública não pode abrir não de suas necessidades legítimas, com intenção de tornar o procedimento licitatório mais abrangente. Fazendo isso o gestor público permitiria que ferramentas mais simples e que atenderiam somente em parte as necessidades da Administração concorressem com soluções integralmente aderentes às necessidades, mais completas e abrangentes. Tal cenário criaria, em última análise, uma situação de desigualdade, visto ser alta a probabilidade das soluções totalmente aderentes às reais necessidades da Administração não conseguirem ser competitivas no certame.

8. INDICAÇÃO DA STIC ESCOLHIDA

Contratação de licenças de acesso a plataforma integrada de treinamento online, na modalidade “Software as Service” (SaaS), especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação, que atenda aos requisitos descritos neste estudo, a saber:

Tema	Característica	Requisito funcional originário	Requisito tecnológico
Conteúdo nativo	Conteúdo em língua portuguesa ou legendado em português nacional (300 itens)	5.1.1. e 5.3.2.	6.1.1.
	Conteúdo LGPD Nacional	5.1.1.	6.1.1.2.
	Entregar conhecimento através de conteúdos tais como: vídeos, games, quizzes, artes (posteres), assessments (avaliações).	5.1.2.	6.1.2.
	Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior)	5.2.2.	6.1.1.1.
Conteúdo do cliente	Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (Moodle, usado pela JE)?	5.1.3.	6.1.5.

	Todas as funcionalidades da plataforma aplicáveis ao conteúdo nativo são aplicáveis ao conteúdo da contratante inserido na plataforma?	5.1.3.	6.1.5.1.
Implantação e segurança	Possui integração com AD?	5.1.8.	6.1.3.5.
	Carga de usuários por meio de arquivos .csv?	5.1.8.	6.1.3.4.
	Permite duplo fator de autenticação para usuários e administradores?	5.5.2.	6.1.3.4.
Normas de segurança como conteúdo	Permite a inclusão dos normativos de segurança da contratante e o aceite pelos usuários? Formato .pdf	5.1.5.	6.1.14.
Automação	Atribuição automática de treinamento para novos usuários?	5.1.9.	6.1.3.2.
	Criação automatizada de um programa personalizado em segurança da informação ou recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários?	5.1.9.	6.1.16.
	APIs que permitam a exportação de todas as informações gerenciais da plataforma de conscientização para base de dados própria da contratante para guarda ou integração com outros sistemas?	5.5.3.	6.1.12. e 6.1.19.
Gestão de usuários e cursos	Seleção de módulos de treinamento para grupo de usuários? (Atribuição de treinamentos).	5.1.7. e 5.1.9.	6.1.3.1.
	Gestão de cursos, tais como: porcentagem de inscrições, cursos iniciados, incompletos, concluídos	5.1.7.	6.1.8.
	Acompanhamento online de progressão e desempenho dos usuários?	5.1.7.	6.1.7.
	Emissão de Certificados para os cursos?	5.1.7.	6.1.11.
	Relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos?	5.1.7.	6.1.10.
	Disparo automático de e-mails de lembrete para usuários com	5.1.7.	6.1.3.3.

	treinamentos pendentes?		
	Inativação de usuários sem perda do histórico de dados?	5.1.7.	6.1.3.6.
	Disponibilizar perfis de acesso para gestão de campanhas e de treinamentos?	5.1.7.	6.1.13.
	Provê ambiente de gestão que possibilita a criação de grupos de usuários com base em comportamento frente às simulações e treinamentos realizados?	5.1.7.	6.1.9.
	Possibilita a atribuição da licença de acesso de um usuário que foi desligado da instituição para um novo usuário (neste caso não é necessário manter o histórico)?	5.1.7.	6.1.3.7.
Campanhas de phishing	Permite a criação de número ilimitado de campanhas durante a vigência do contrato?	5.1.4.	6.1.15.1.
	Disponibiliza pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos pela contratante?	5.1.4.	6.1.15.2.
	Mantem histórico por usuário e por campanha?	5.1.4.	6.1.15.3.
	Permite que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação?	5.1.4.	6.1.15.4.
Indicador de maturidade em segurança	Possui indicador de nível de risco em segurança da informação para cada usuário e para a instituição? O nível de risco deve ser medido considerando-se pelo menos dois fatores: participação em treinamentos e avaliação nos testes de phishing.	5.1.6.	6.1.17.
Suporte técnico	A contratada disponibiliza durante todo período contratual um gerente de contas para apoiar e orientar a contratante no uso da plataforma, com as atribuições previstas no item 6.2.1?	5.3.1.	6.2.1/ 6.2.2./ 6.2.4.
	Repasse de conhecimento	5.2.1.	6.2.3.
Customização	Permite inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários?	5.2.3.	6.1.4.

Linguagem da plataforma	Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br)	5.2.4.	6.1.18.

*Alinhamento entre requisitos funcionais e tecnológicos

9. QUANTITATIVO A SER CONTRATADO

Item	Descrição	CATSER	Unidade de medida	Qtde. Estimada
1	Licenças de acesso a plataforma integrada de treinamento online, na modalidade "Software as Service" (SaaS), especializada em oferta de conteúdos de capacitação e conscientização em segurança da informação, pelo período de 36 (trinta e seis) meses.	26077	UN	1000

10. ESTRATÉGIA DA CONTRATAÇÃO

Considerando que o quadro de servidores (em sentido amplo) do TRE-AM pode sofrer variação, sugere-se que a contratação seja realizada por meio de Ata de Registro de Preços, nos termos do art. 3º, inciso II, do Decreto nº 7.892/2013.

11. VALOR ESTIMADO DA CONTRATAÇÃO

Estima-se a presente contratação em R$ 299.000,00 (duzentos e noventa e nove mil reais).

12. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica, visto que se trata de item único.

13. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

A contratação em tela não requer providências prévias da Administração quanto a capacitação de servidores ou de empregados para fiscalização e gestão contratual ou adequação do ambiente da organização (infraestrutura tecnológica, mobiliário, espaço físico etc.).

14. ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

14.1. Gestão da plataforma de conscientização

Haverá necessidade de gestão da plataforma em relação aos treinamentos e às campanhas de phishing. Desde a concepção, essa contratação integra as equipes de Recursos Humanos e Tecnologia da Informação

tendo, inclusive, servidores dessas duas áreas na elaboração dos artefatos de planejamento da contratação. Na execução do programa, é altamente recomendável que:

- A gestão dos treinamentos fique a cargo da área de recursos humanos com apoio da área Tecnologia da Informação, no que tange a construção do programa de capacitação em Segurança da Informação;
- A gestão de eventuais treinamentos a serem adicionados na plataforma fique a cargo da área de recursos humanos;
- A gestão das campanhas de phishing fiquem a cargo da área de Tecnologia da Informação.

A gestão da plataforma terá sempre o apoio do Gerente de Contas da Contratada, conforme atribuições definidas neste documento de planejamento.

14.2. Gestão do Programa de Conscientização em Segurança da Informação

É altamente recomendável que as áreas de Gestão de Pessoas e Tecnologia da Informação definam um cronograma de treinamentos e testes de phishing, com periodicidade máxima semestral, e busque o apoio da alta administração para efetivar a execução junto aos usuários finais.

15. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não há contratação correlata em andamento.

16. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS DE TRATAMENTO

A contratação em tela não implica em impactos ambientais significativos a demandar ações por parte da contratante ou da contratada.

17. POSICIONAMENTO CONCLUSIVO SOBRE A VIABILIDADE E RAZOABILIDADE DA CONTRATAÇÃO

Ante o exposto, esta Equipe de Planejamento da Contratação conclui pela viabilidade da contratação de licenças de acesso a plataforma integrada de treinamento online, na modalidade “Software as Service” (SaaS), especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação, pelo período de 36 (trinta e seis) meses.

Manaus, 01 de agosto de 2023.

Equipe de Planejamento da Contratação (Portaria TRE-AM nº 370/2023):

Rubens Antônio Pinto Soares
Requisitante/ Integrante Técnico

Isaías Araújo Lima Filho
Integrante Técnico

Euzébio Rodrigues Cardoso Júnior
Integrante Administrativo

Em 13 de novembro de 2023.

Em 13 de novembro de 2023.

Documento assinado eletronicamente por **EUZEBIO RODRIGUES CARDOSO JUNIOR**, **Analista Judiciário**, em 13/11/2023, às 13:27, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **RUBENS ANTONIO PINTO SOARES**, **Técnico Judiciário**, em 13/11/2023, às 15:14, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-am.jus.br /sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0000107838** e o código CRC **3858FB0B**.