TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra, 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

DOD-ADMINISTRATIVO - GAB-SAO/2024

Modelo atualizado em: 25/03/2024
SEI nº 0007932-30.2024.6.08.8000

PREENCHIMENTO PELA ÁREA ADMINISTRATIVA

1. INFORMAÇÃO SOBRE A PREVISÃO NO PLANO DE CONTRATAÇÕES DE TIC

Demanda prevista no Plano de Contratações de STIC 2025, item ES14.

2. INDICAÇÃO E CIÊNCIA DOS INTEGRANTES ADMINISTRATIVOS (TITULAR E SUBSTITUTO)

(IDENTIFIQUE OS INTEGRANTES ADMINISTRATIVOS. OS INTEGRANTES ADMINISTRATIVOS DEVERÃO DAR **CIÊNCIA** NESTE DOCUMENTO)

Nome do Titular : José Adriani Brunelli Desteffani

Nome do Substituto : Carlos Alberto da Rocha Pádua Filho

3. INDICAÇÃO E CIÊNCIA DOS FISCAIS ADMINISTRATIVOS (TITULAR E SUBSTITUTO)

(IDENTIFIQUE OS FISCAIS ADMINISTRATIVOS. OS FISCAIS ADMINISTRATIVOS DEVERÃO DAR **CIÊNCIA** NESTE DOCUMENTO)

Nome do Titular : José Adriani Brunelli Desteffani

Nome do Substituto : Carlos Alberto da Rocha Pádua Filho

3. ENCAMINHAMENTO

Senhor Diretor Geral,

Encaminho os presentes autos para formalização e instituição das Equipes de Planejamento e de Gestão Contratual, em atendimento ao art. 17, §3º, da Resolução TRE 63/2023.

ESTUDO TÉCNICO PRELIMINAR (TIC) Nº 03/2025 - TRE-ES/PRE/DG/STI/CIS/NSC

(este documento deve seguir as orientações da Resolução TRE/ES n. 63/2023)
Modelo atualizado em: 29/04/2024
SEI nº 0007932-30.2024.6.08.8000

SEÇÃO I - ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. IDENTIFICAÇÃO DA SOLUÇÃO SOLICITADA

Renovação de licenças de acesso à plataforma integrada de treinamento online, especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação KnowBe4.

1.1. DESCRIÇÃO

Renovação de serviço de conteúdo na modalidade “Software as Service” (SaaS) para treinamento usuários de TIC, por meio do acesso à plataforma online (KnowBe4), especializada na oferta de conteúdos de capacitação e conscientização em Segurança da Informação.

1.2. MOTIVAÇÃO E RESULTADOS A SEREM ALCANÇADOS

As pessoas são o elo mais fraco quando falamos em segurança cibernética. Costumam ser a porta de entrada para criminosos cibernéticos invadirem a rede, roubarem informações valiosas e causarem grandes prejuízos financeiros e de imagem às instituições. Treinar e conscientizar pessoas é primordial para o fortalecimento da segurança da infraestrutura tecnológica e dos dados pessoais.

A contratação de solução para conscientização em segurança da informação está prevista na Estratégia Nacional de Cibersegurança da Justiça Eleitoral (processo SEI 0005695-28.2021.6.08.8000), Anexo I - Arquitetura de Ciber Segurança, 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.

Em 2022 o TRE-ES contratou a ferramenta KnowBe4 para permitir a criação de treinamentos visando a conscientização em segurança da informação de servidores, requisitados, estagiários e terceirizados, além de permitir a criação de campanhas de phishing. A plataforma KnowBe4 permitiu a realização de 5 campanhas de treinamento, mais de 40 campanhas de phishing e inclusão de 13 Normas de Segurança da Informação para ciência dos usuários. Esta contratação foi oriunda de uma Ata de Registro de Preços para todos os Tribunais da Justiça Eleitoral participantes, a presente renovação também deverá permtir a participação de Tribunais da Justiça Eleitoral interessados.

A utilização da plataforma KnowBe4 tem permitido o acompanhamento do nível de risco dos usuários com base em suas ações com relação a treinamentos e e-mails de phishing, gerando também um índice geral como nível de risco de todo o TRE-ES. A aceitação dos usuários para os treinamentos tem sido alta, tendo obtido avaliações dos treinamentos realizados pelos usuários com médias de 4.8 em uma escala de 0.0 até 5.0. As políticas de segurança da informação estão todas publicadas na plataforma, permitindo sua atualização constante e o acesso dos usuários sempre que desejarem. A plataforma ainda auxilia no direcionamento de e-mails em campanhas de phishing para usuários e permite o controle dos cliques realizados, permitindo o direcionamento de novos treinamentos.

Em 19/07/2023 foi aprovado o Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES, que prevê ações de capacitação e conscientização em segurança cibernética, ampliando a utilização da ferramenta KnowBe4, de forma a atender ao estabelecido no programa.

A contratação em tela pretende alcançar aos seguintes resultados:

- Aumentar a maturidade em segurança cibernética dos servidores, requisitados, estagiários e terceirizados;

- Reduzir o risco da Organização por meio da orientação dos usuários sobre segurança física, segurança de links, senhas, phishing e normas;

- Reduzir o risco relacionado a e-mails de phishing, por meio de simulações com os usuários orientando-os sobre como agir;

- Manter a disponibilização das normas em local adequado permitindo o registro da ciência de todos os usuários; e

- Atender ao Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES.

2. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

2.1. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

Como um dos pilares para a execução de um programa permanente de conscientização em segurança da informação na Justiça Eleitoral, a solução deve prover, no mínimo, os seguintes recursos:

2.1.1 - Disponibilizar ampla biblioteca de conteúdos de segurança da informação, inclusive LGPD, em língua portuguesa.

2.1.2 - Entregar conhecimento com uso de recursos interativos, como vídeo, simulações, quizzes (questionários rápidos), boletins informativos, etc.

2.1.3 - Possibilitar a inclusão de cursos produzidos pela própria Justiça Eleitoral ou por terceiros, gerenciando-os juntamente com os conteúdos nativos da solução.

2.1.4 - 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).

2.1.5 - 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.

2.1.6 - Permitir acompanhamento da evolução da maturidade dos usuários e da instituição em relação à Segurança da Informação.

2.1.7 - Permitir a gestão completa de treinamento e usuários.

2.1.8 - Permitir integração com a base de dados de usuários da instituição.

Fig. 1 - Requisitos de negócio estruturantes da solução.

2.1.9 - Para essa contratação é premissa que a plataforma permita automatização de tarefas, tendo em vista a necessidade de racionalização de recursos humanos da Justiça Eleitoral. Atribuição automática de treinamentos, agendamento de campanhas de phishing, apoio técnico na execução do programa de conscientização através da plataforma são fatores fundamentais para o atingimento dos objetivos propostos.

2.1.10 - Utilização de inteligência artificial para auxiliar na criação de templates de phishing personalizados; atribuição de treinamentos personalizados com base no nível de risco do usuário; e elaboração de questionários sobre as normas de segurança do TRE-ES, de forma a garantir que os usuários entenderam os termos para os quais deram ciência.

2.2. IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

2.2.1. 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:

2.2.1.1 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

2.2.1.2 Deve haver conteúdo específico voltado a LGPD Brasileira.

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

2.2.3. Prover gerenciamento de usuários e cursos, permitindo:

2.2.3.1 - Seleção de módulos de treinamento para grupo de usuários;

2.2.3.2 - Atribuição automática de treinamentos para novos usuários;

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

2.2.3.4 - Carga de usuários por meio de arquivo .CSV;

2.2.3.5 - Integração com o AD (Active Directory) da contratante;

2.2.3.6 - Inativação de usuários sem perda do histórico de dados;

2.2.3.7 - 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.

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

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

2.2.5.1 - Todas as funcionalidades de gestão disponíveis para os conteúdos nativos devem poder ser aplicadas aos conteúdos próprios da contratante;

2.2.6 - Permitir a carga e o aceite de políticas e normas de segurança da informação da contratante;

2.2.7. Prover ambiente de gestão para acompanhamento online de progressão e desempenho dos usuários;

2.2.8. Disponibilizar detalhes sobre a porcentagem de inscrições, cursos iniciados, incompletos, concluídos e conhecimento da política de segurança e normas;

2.2.9. Prover ambiente de gestão que possibilite a criação de grupos de usuários com base em comportamento frente às simulações e treinamentos realizados;

2.2.10. Disponibilizar relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos.

2.2.11. Permitir a emissão de certificados para os treinamentos.

2.2.12. Prover APIs de relatórios que permitam personalizar os documentos, integrando-os a outros sistemas de negócios para apresentar os dados a partir da plataforma.

2.2.13. Disponibilizar perfis de acesso para gestão de campanhas e treinamentos (desejável também perfil para auditoria, porém não obrigatório);

2.2.14. Possibilitar a autenticação em dois fatores para usuários e administradores;

2.2.15, Possibilitar a criação de campanhas simuladas de phishing, a fim de avaliar o comportamento dos usuários;

2.2.15.1. Permitir criação de número ilimitado de campanhas durante a vigência do contrato;

2.2.15.2. Disponibilizar pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos diretamente pela contratante;

2.2.15.3. Manter histórico por usuário e por campanha;

2.2.15.4. Permitir que os usuários seja testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação.

2.2.16 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.

2.2.17. 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.

2.2.18. Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br).

2.2.19. 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.

2.2.20. 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:

2.2.20.1. Acompanhar o projeto (programa de conscientização);

2.2.20.2. Esclarecer dúvidas;

2.2.20.3. Sugerir proativamente novos caminhos para o programa;

2.2.20.4. Ser ponte com o suporte técnico.

2.2.20.5. Configurar a conta e fazer a integração com a infraestrutura da contratante (*onboarding*).

2.2.21. As atividades do gerente de contas podem ser desenvolvidas remotamente, com uso de meios de comunicação digital

2.2.22. 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:

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

2.2.22.2. Configuração da integração com Active Directory e ADFS;

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

2.2.22.4. Habilitação de Duplo Fator de Autenticação.

2.2.23. 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*.

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

1. Melhores práticas para implantação;
2. Forma de Acesso dos usuários e download de conteúdos;
3. Criação de grupos inteligentes;
4. Atribuição de treinamentos a grupos de usuários;
5. Carga de conteúdos da contratante;
6. Criação e automatização de campanhas de phishing;
7. Criação de *roles* (papeis) de segurança;
8. Carga, inativação e exclusão de usuários;
9. Personalização de identidade visual;
10. Emissão e extração de relatórios;

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

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

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

2.3. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

2.3.1 - 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 em sigilo 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.

2.3.2 - Garantir a segurança das informações dos usuários carregadas na plataforma.

2.3.3 - 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 o âmbito do CONTRATO o compartilhamento de dados pessoais ou dados pessoais sensíveis com a CONTRATADA.

2.4. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

2.4.1 - Durante todo o período de contrato deve haver um profissional especializado apto a prestar suporte aos gestores da plataforma no esclarecimento de dúvidas. O profissional deve estar acessível no período 8hx5d, dias úteis.

2.4.2 - A contratada deve garantir o quantitativo mínimo de treinamentos estabelecido neste Estudo Técnico.

3. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

A demanda dos demais Tribunais Eleitorais é apresentada na tabela abaixo, juntamente com as informações do documento que formalizou a participação na Ata de Registro de Preços.

DEMANDA DOS TRIBUNAIS		
Tribunal	**Quantidade**	**Formalização**
STM	1732	Ofício nº 4237670 (1353106)
TRE/AC	250	Ofício nº 22/2025 (1345903)
TRE/AL	500	Ofício nº 503/2025 (1345898)
TRE/AP	330	Ofício nº 294 / 2025 (1340606)
TRE/BA	2000	Ofício nº 288/2025 (1336125, 1336127, 1336132, 1336470)
TRE/CE	1650	Ofício nº 370/2025 (1339703)
TRE/DF	800	Ofício nº 204 / 2025 (1339092)
TRE/ES	570	Processo SEI 0007932-30.2024.6.08.8000
TRE/GO	1500	Ofício nº 45/2025 (1343682)
TRE/MA	1300	Ofício nº 1656 / 2025 (1349792)
TRE/MG	3500	Ofício nº 412/2025 (1346591)
TRE/MS	700	Ofício nº 507 / 2025 (1340302, 1340307)
TRE/MT	700	Ofício nº 15/2025 (1341404)
TRE/PA	1185	Ofício nº 485/2025 (1343184)
TRE/PB	1000	Ofício nº 10/2025 (1341813)
TRE/PE	1267	Ofício nº 1750/2025 (1343689)
TRE/PI	765	Ofício nº 4/2025 (1346231)
TRE/PR	2000	Ofício n.º 121/2025 (1339098)
TRE/RJ	2000	Ofício nº 27/2025 (1341395)
TRE/RO	550	Ofício nº 24/2025 (1348630)
TRE/RR	300	Ofício nº 440/2025 (1344618, 1344622, 1344626)

TRE/RS	1500	Ofício nº 949/2025 (1338208, 1338215)
TRE/SC	1100	Ofício nº 361,2025 (1345570)
TRE/SE	600	Ofício nº 436/2025 (1341640)
TRE/SP	5200	Ofício nº 301/2025 (1346608)
TRE/TO	700	Ofício nº 514 / 2025 TRE-TO (1337997)
TSE	2500	Ofício nº 86/2025 (1344944, 1344945, 1344946, 1344947, 1344948)
TOTAL	**36.199**	

Tabela 1 - Demanda dos Tribunais

Em relação a necessidade deste TRE/ES, o quantitativo será destinado aos usuários conforme tabela abaixo:

TIPO	TOTAL
ESTAGIÁRIOS	58
EFETIVOS	309
REQUISITADOS	111
TERCEIRIZADOS	55
REMOVIDOS PARA TRE-ES	16
SEM VÍNCULO EFETIVO	12
MEMBROS ATIVOS	8
LOTAÇÃO PROVISÓRIA	1
	570

Tabela 2 - Demanda do TRE/ES

- A equipe de planejamento entende que os preços devem ser registrados através de uma ARP para que cada Tribunal, de acordo com o seu planejamento, decida sobre o momento mais apropriado para a contratação dentro do prazo de validade da Ata.
- A equipe entende que a ARP deve ser aberta para adesão tardia (caronas) SOMENTE para a Justiça Eleitoral, tendo em vista que os pilares do programa de conscientização que originaram as especificações técnicas deste Estudo foram definidos por grupo nacional constituído pelo TSE. O TSE e todos os Tribunais Regionais foram consultados. Somente o TRE/AM optou por não participar neste momento, sendo, portanto, a adesão tardia limitada a este Tribunal.
- Em relação à participação de outros órgãos, para que não haja atraso no processo de contratação, o que ocasionaria o término da vigência das licenças atuais e a consequente inativação dos usuários, essa poderá ocorrer somente em fase de elaboração dos estudos técnicos preliminares e minuta de termo de referência, desde que o órgão interessado cumpra os requisitos obrigatórios e envie, para instrução processual, o estudo técnico que concluí pela contratação da mesma ferramenta que está sendo contratada pela Justiça Eleitoral.

4. ANÁLISE DAS POSSÍVEIS SOLUÇÕES

No atual cenário da Justiça Eleitoral, quase a totalidade dos Tribunais já utiliza a solução KnowBe4, que vem apresentando excelentes resultados para promoção da conscientização dos usuários de recursos de TIC da Justiça Eleitoral em conceitos de segurança da informação. A plataforma é comercializada no formato de licença por usuário nos níveis Prata (treinamentos nível I), Ouro (treinamentos nível I e II), Platina (treinamentos nível I e II) e Diamante (treinamentos nível I, II e III), sendo o nível Diamante o atualmente contratado, por possuir maior quantidade de treinamentos em língua portuguesa, conforme tabela abaixo:

contagem geral de componentes de treinamento em Português Brazil			
Training Content	Level I	Level II	Level III
Training Modules	14	33	151
Mobile First Modules	3	14	74
Video Modules	16	26	331
Games	3	5	14
Posters / Images	18	24	93
Newsletters / Documents	15	30	115
Assessments	3	3	3
Total Pieces of Content	72	135	781

Tabela 3 - Quantitativo de treinamentos KnowBe4

A plataforma agora também fornece um módulo chamado AIDA: Inclui modelos de phishing gerados por IA, treinamento automatizado, questionários de políticas e atualizações de conhecimento, o que facilita no direcionamento de treinamentos e simulações de phishing de acordo com o nível de risco dos usuários e as áreas de conhecimento que precisa mais.

4.1. IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	KnowBe4 - Licença Diamond com AIDA por 36 meses

4.2. ANÁLISE COMPARATIVA DAS SOLUÇÕES

a) Solução similar que possa ser disponibilizada por outro órgão ou entidade da Administração Pública;

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

c) S*oftware* livre ou *software* público.

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

d) **Solução de mercado, comercial.**

Avaliação de plataforma para programa permanente de conscientização em segurança da informação.			
Tema	**Característica**	**Item do ETP**	**KnowBe4**
Conteúdo Nativo	Conteúdo em língua portuguesa ou legendado em português nacional (300 itens)	2.2.1	Sim (781)
	Conteúdo LGPD Nacional	2.2.1.2	Sim
	Entregar conhecimento através de conteúdos tais como: vídeos, games, quizzes, artes (posteres), assessments (avaliações).	2.2.2	Sim
	Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior)	2.2.1.1	Sim
Conteúdo do	Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (Moodle, usado pela JE)?	2.2.5	Sim

Cliente	Todas as funcionalidades da plataforma aplicáveis ao conteúdo nativo são aplicáveis ao conteúdo da contratante inserido na plataforma?	2.2.5.1	Sim
Implantação e Segurança	Possui integração com AD?	2.2.3.5	Sim
	Carga de usuários por meio de arquivos csv?	2.2.3.4	Sim
	Permite duplo fator de autenticação para usuários e administradores?	2.2.14	Sim
Normas de Segurança como conteúdo	Permite a inclusão dos normativos de segurança da contratante e o aceite pelos usuários? Formato PDF.	2.2.5 e 2.2.6	Sim
Automação	Atribuição automática de treinamento para novos usuários?	2.2.3.2	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?	2.2.16	Sim
	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?	2.2.12 e 2.2.19	Sim
Gestão de Usuários e Cursos	Seleção de módulos de treinamento para grupo de usuários? (Atribuição de treinamentos).	2.2.3.1	Sim
	Gestão de cursos, tais como: porcentagem de inscrições, cursos iniciados, incompletos, concluídos	2.2.8	Sim
	Acompanhamento online de progressão e desempenho dos usuários?	2.2.7	Sim
	Emissão de Certificados para os cursos?	2.2.11	Sim
	Relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos?	2.2.10	Sim
	Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes?	2.2.3.3	Sim
	Inativação de usuários sem perda do histórico de dados?	2.2.3.6	Sim
	Disponibilizar perfis de acesso para gestão de campanhas e de treinamentos?	2.2.13	Sim
	Provê ambiente de gestão que possibilita a criação de grupos de usuários com base em comportamento frente às simulações e treinamentos realizados?	2.2.9	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)?	2.2.3.7	Sim
Campanhas de Phishing	Permite a criação de número ilimitado de campanhas durante a vigência do contrato?	2.2.15.1	Sim
	Disponibiliza pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos pela contratante;	2.2.15.2	Sim
	Mantem histórico por usuário e por campanha	2.2.15.3	Sim

	Permite que os usuários seja testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação?	2.2.15.4	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.	2.2.17	Sim
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 3.20?	2.2.20, 2.2.21, 2.2.24	Sim
	Passagem de Conhecimento	2.2.23	Sim
Customização	Permite inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários?	2.2.4	Sim
Linguagem da Plataforma	Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br)	2.2.18	Sim

Tabela 4 - Comparativo de soluções de mercado.

4.3. ESTIMATIVA DE CUSTOS PARA CADA SOLUÇÃO

Id	Descrição da solução (ou cenário)
1	KnowBe4 - Licença Diamond + AIDA por 36 meses : R$ 106,48 por usuário

Conforme Proposta da Qualitek documento 1349871.

5. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Não se aplica.

6. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Não se aplica.

6.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

1. Solução Viável 1

a) Descrição da solução 1: KnowBe4 - Licença Diamond com AIDA por 36 meses

b) Custo Total de Propriedade da solução 1 – Memória de Cálculo

Item	Unidade	Quantidade	Valor Unitário	Valor Total
Diamond	pessoa	570	R$ 106,48	R$ 60.693,60

6.2. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos			
	Ano 1	Ano 2	Ano 3	Total
Solução Viável 1	R$ 60.693,60	R$ 0,00	R$ 0,00	**R$ 60.693,60**

7. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Solução de mercado, comercial.

KnowBe4 - Licença Diamond com AIDA por 36 meses.

7.1. ANÁLISE DA DEPENDÊNCIA TECNOLÓGICA

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.

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:

1. Certificados de conclusão dos Cursos.
2. Avaliação de maturidade em segurança dos usuários e da instituição;
3. Conteúdos da contratante disponibilizados na plataforma.
4. Aceite das normas de segurança da informação.

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.

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.

7.2. COMPOSIÇÃO DE BENS ou SERVIÇOS DA SOLUÇÃO

Serviço. Software como serviço. Licenças de uso por período determinado, na infraestrutura na nuvem.

7.3. INDICAÇÃO DA NECESSIDADE DE PARCELAMENTO DO OBJETO

Não se aplica.

8. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Estimativa de Custo	Quantidade	Valor Unitário	Valor Total
TRE-ES	570	R$ 106,48	R$ 60.693,60
ARP	**36.199**	R$ 106,48	R$ 3.854.469,52

9. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Declaramos que a solução KnowBe4 - Licença Diamond com AIDA por 36 meses é viável porque atende todos os requisitos especificados no item 2 e traz os seguintes benefícios:

- Manutenção dos dados históricos dos usuários no uso da plataforma, com seus respectivos riscos calculados;
- Registro dos cursos e e-mails já utilizados em treinamentos e campanhas de phishing;

- Manutenção do Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES;

- Garantia da qualidade dos treinamentos realizados;

- Manutenção das normas de segurança da informação em uma plataforma para registrar a ciência dos usuários e facilitar o acesso;

- Manutenção do sistema de reportar phishing utilizando o PAB (botão para reportar phishing da plataforma) para manutenção dos indicadores do TRE-ES; e

- Possibilidade de utilização da AIDA (inteligência artificial da plataforma) para direcionamento de treinamentos e campanhas de phishing.

SEÇÃO II - ANÁLISE DE SUSTENTAÇÃO E TRANSIÇÃO CONTRATUAL

1. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

1.1. Recursos Materiais

Não há.

1.2. Recursos Humanos

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 documentos 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 ao atendimento do Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES;
- A gestão de eventuais treinamentos adicionais adicionados 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.

2. ESTRATÉGIA DE CONTINUIDADE CONTRATUAL

2.1 – Ações de Continuidade, seus respectivos responsáveis e prazos

Início do processo de prorrogação/renovação contratual 6 meses antes do término do contrato atual, conforme Resolução TRE-ES 63/2023.

3. ESTRATÉGIA DE TRANSIÇÃO CONTRATUAL

Conforme Item 7.1 deste estudo, todas as informações gerenciais devem ser exportadas ao longo do contrato para continuidade do Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES no caso de descontinuidade do fornecimento.

4. ESTRATÉGIA DE INDEPENDÊNCIA

Conforme Item 7.1 deste estudo, todas as informações gerenciais devem ser exportadas ao longo do contrato para continuidade do Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES no caso de descontinuidade do fornecimento.

SEÇÃO III - MAPA DE GERENCIAMENTO DE RISCOS

1. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

A tabela a seguir apresenta uma síntese dos riscos identificados e classificados:

Id	Risco	Relacionado ao (à): (*)	P (**)	I (***)	Nível de Risco (P × I) (****)
1	Atraso no trâmite processual	Planejamento da Contratação	2	3	6
2	Exposição de informações de maturidade em segurança da informação	Incidente de Segurança da Informação	2	4	8
3	Inexecução contratual	Gestão Contratual	2	3	6
4	Baixa participação nos treinamentos	Gestão do Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES	3	4	12

Legenda: P = Probabilidade; I = Impacto.
* A qual natureza o risco está associado: fases do Processo da Contratação ou Solução Tecnológica: Planejamento, Seleção do Fornecedor, Gestão do Contrato.
** **Probabilidade**: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000). Usualmente usa-se uma escala de 1 a 5, sendo 1= muito baixo, 2= baixo, 3= médio, 4= alto, 5= muito alto.
*** **Impacto**: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009). Usualmente usa-se uma escala de 1 a 5, sendo 1= muito baixo, 2= baixo, 3= médio, 4= alto, 5= muito alto.
**** **Nível de Risco**: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009). Obtido pelo produto da probabilidade pelo impacto.

Id	Risco	Relacionado ao(à):	P	I	Nível de Risco (P × I)
R01	Atraso no trâmite processual	Planejamento da Contratação	2	3	6
R02	Exposição de informações de maturidade em segurança da informação	Incidente de Segurança da Informação	3	2	6
R03	Inexecução contratual	Gestão Contratual	4	4	16
R04	Baixa participação nos treinamentos	Gestão do Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES	2	3	6

2. AVALIAÇÃO E TRATAMENTO DOS RISCOS IDENTIFICADOS

Risco 01:	Atraso no trâmite processual	
Probabilidade:	Baixa	
Impacto:	Médio	
Dano 1:	Não continuar o Programa de Conscientização e Capacitação em Segurança da Informação do TRE-ES	
Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Consultar empresas do ramo sobre adequação das especificações técnicas às características dos equipamentos fornecidos pelo mercado.	Integrante Técnico
P2	Verificar/adequar/sugerir questões sobre os aspectos administrativos da contratação	Integrante administrativo
Id	**Ação de Contingência**	**Responsável**
C1	Aplicar treinamentos avulsos voltados a Segurança da Informação	STI e SGP

Risco 02:	EXPOSIÇÃO DE INFORMAÇÕES DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO	
Probabilidade:	Baixo	
Impacto:	Alto	
Dano 1:	Uso das informações para ações de engenharia social visando comprometer a infraestrutura tecnológica	
Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Inserir no termo de referência a necessidade de duplo fator de autenticação para acesso à plataforma	Integrante Técnico

Risco 03:	INEXECUÇÃO CONTRATUAL	
Probabilidade:	Baixo	
Impacto:	Médio	
Dano 1:	Interrupção do Programa de treinamento continuado.	
Dano 2:	Indisponibilidade das informações gerenciais de maturidade.	
Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Inserir no termo de referência a necessidade de APIs para exportação dos dados gerenciais.	Integrante Técnico

Risco 04:	BAIXA PARTICIPAÇÃO NOS TREINAMENTOS	
Probabilidade:	Média	
Impacto:	Alto	
Dano 1:	Baixo crescimento da maturidade em Segurança da Informação	
Dano 2:	Aumento do risco de um incidente de segurança da informação	
Tratamento:	Mitigar.	
Id	**Ação Preventiva**	**Responsável**
P1	Integrar as equipes de TIC e SGP na gestão do programa e da plataforma contratada	Fiscais Técnicos (SGP e STI)
P2	Buscar Apoio da Alta Administração para aprovação de um cronograma de execução de treinamentos para todos os usuários.	SGP e STI
P3	Criar equipe Nacional para elaboração de um programa padrão com base na plataforma que poderá ser usado por todos os Tribunais.	TSE
Id	**Ação de Contingência**	**Responsável**

3 – ACOMPANHAMENTO DAS AÇÕES DE TRATAMENTO DE RISCOS

Data	Id. Risco	Id. Ação	Registro e acompanhamento das ações de tratamento dos riscos
09/12/2024	R01	P1	Consulta à KnowBe4 para dirimir dúvidas sobre a renovação contratual.

4 – APROVAÇÃO E ASSINATURA

Equipe de **Planejamento da Contratação** (Portaria 1312159)	
Integrantes Demandantes	Sandro Merçon da Silva (titular) Olga Bayerl Vita (substituto)
Integrantes Técnicos	Olga Bayerl Vita (titular) Carlos Eduardo Laquine (substituto)
Integrantes Administrativos	José Adriani Brunelli Desteffani (titular) Carlos Alberto da Rocha Pádua Filho (substituto)

Vitória, 20 de março de 2025.

Documento assinado eletronicamente por **SANDRO MERÇON DA SILVA**, **Coordenador(a)**, em 20/03/2025, às 15:02, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOSE ADRIANI BRUNELLI DESTEFFANI**, **Secretário(a)**, em 20/03/2025, às 15:07, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **OLGA BAYERL VITA**, **Assistente do Núcleo de Segurança Cibernética**, em 20/03/2025, às 15:26, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1353592** e o código CRC **F7C9D7C3**.