



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

ESTUDO TÉCNICO PRELIMINAR (DEMANDAS DE TIC) Nº 08/2022 V2 - TRE-ES/PRE/DG/STI/CIS

(este documento deve seguir as orientações da Resolução TRE/ES nº 261/2018)

SUMÁRIO

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO.

1. Caracterização da Demanda.
2. Especificação dos Requisitos Funcionais.
3. Especificação dos Requisitos Técnicos Mínimos.
4. Identificação e Comparação das Soluções Aderentes aos Requisitos.
5. Indicação da STIC Escolhida.
6. Indicação da Necessidade de Adequação Ambiental

ANÁLISE DE RISCOS.

7. Identificação dos Riscos.
8. Relação dos Riscos e Ações de Mitigação.

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO.

9. Recursos Materiais e Humanos.
10. Descontinuidade do Fornecimento.

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. CARACTERIZAÇÃO DA DEMANDA

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

1.1 DESCRIÇÃO SUCINTA

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

1.2 JUSTIFICATIVA DA NECESSIDADE E RESULTADOS

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.

1. Conforme repassado aos Diretores Gerais e Secretários de TIC pelo sr. Secretário de TIC do TSE, Júlio Valente, as contratações previstas na Estratégia Nacional serão planejadas por grupos de até 4 (quatro) Tribunais Regionais Eleitorais

para atender a Justiça Eleitoral do país, inclusive o TSE.

2. Em relação a esta contratação, ficou estabelecido que o TRE/ES conduzirá o processo administrativo de contratação como orgão gerenciador, com apoio dos TREs do DF, GO e TO na elaboração dos documentos de planejamento.
3. O processo em curso contemplará, além das necessidades do TRE/ES, as demandas de todos os demais Tribunais Eleitorais interessados, que integrarão a contratação como partícipes desde a origem. O produto final do procedimento administrativo deverá ser uma ata de registro de preços para utilização por todos os partícipes.
4. Em consonância com o Decreto 7.892/2013, Art. 6º, I, a inclusão no registro de preços deve estar formalizada e aprovada pela autoridade competente de cada Tribunal. Assim, durante a fase de planejamento da contratação foram encaminhados ofícios da Diretoria Geral deste Tribunal aos demais Regionais e ao TSE, questionando sobre a efetiva participação e sobre o quantitativo a ser incluído nos documentos de planejamento. Toda a documentação comprobatória integra do processo SEI TRE/ES nº 0001048-53.2022.6.08.8000. Os quantitativos de cada Regional estão previstos do item **RELAÇÃO ENTRE DEMANDA PREVISTA E A STIC**.

A contratação supre também recomendação do TCU, inicialmente direcionada ao TSE, no Acórdão 3143/2021 - SEI 0678959, 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, em: 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. 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.

O resultado desta contratação será um crescimento acentuado da maturidade dos usuários de TIC da Justiça Eleitoral em relação à Segurança da Informação.

2. ESPECIFICAÇÃO DOS REQUISITOS FUNCIONAIS

REQUISITOS RELACIONADOS AO NEGÓCIO

A fim de tornar-se 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 - Disponibilizar ampla biblioteca de conteúdos de segurança da informação, inclusive LGPD, em língua portuguesa.

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

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

2.4 - 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).

2.5 - 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.

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

2.7 - Permitir a gestão completa de treinamento e usuários.

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

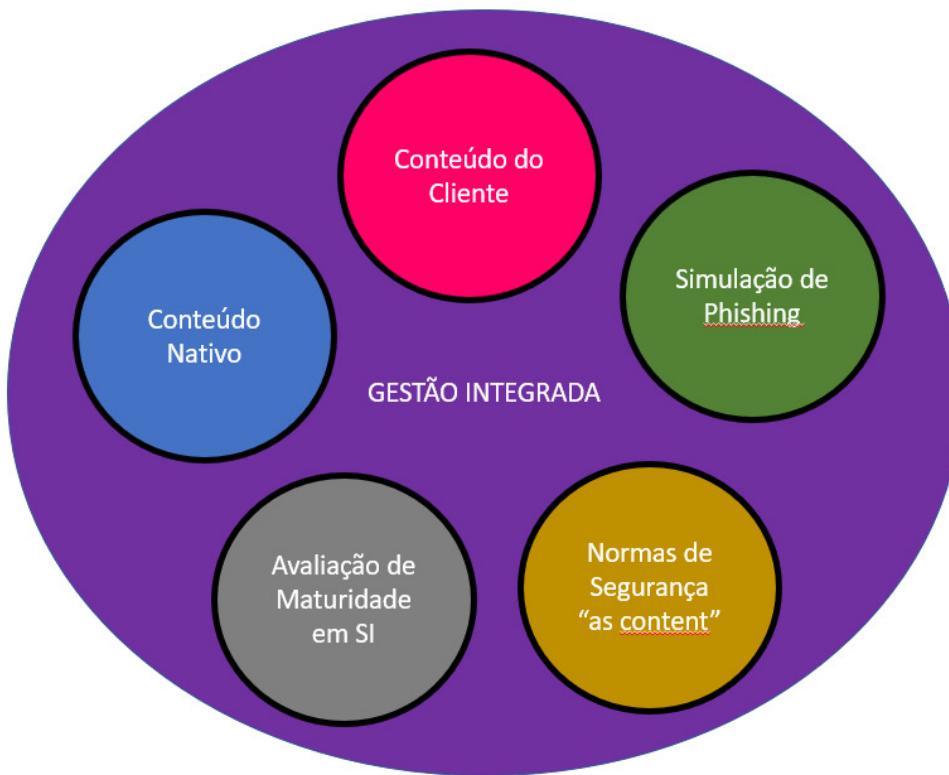


Fig. 1 - Requisitos de negócio estruturantes da solução.

2.9 - 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.

REQUISITOS DE CAPACITAÇÃO, AMBIENTAIS, CULTURAIS E SOCIAIS

2.10 - Deve haver uma instrução no modelo *hands-on* para os gestores da plataforma.

2.11 - Deve possuir conteúdo acessível à deficientes auditivos e visuais.

2.12 - Permitir a inclusão da identidade visual da instituição nas campanhas e treinamentos.

2.13 - Ambiente da plataforma deve ser disponibilizado totalmente em português.

REQUISITOS DE MANUTENÇÃO E GARANTIA

2.14 - 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.

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

REQUISITOS TEMPORAIS

2.16. - O mercado, em geral, oferece licenças de acesso pelo período de 1 (um) ano a 3 (três anos). No caso da Justiça Eleitoral, tendo em vista a necessidade de estabelecimento de um programa permanente de conscientização, conforme preconiza o Acórdão TCU 3143/2021, 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 anos.

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

REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

2.18 - 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.

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

2.20 - 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.

3. ESPECIFICAÇÃO DOS REQUISITOS TÉCNICOS MÍNIMOS.

A. CARACTERÍSTICAS GERAIS

3.1. 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:

3.1.1 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

3.1.2 Deve haver conteúdo específico voltado a LGPD Brasileira.

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

3.3. Prover gerenciamento de usuários e cursos, permitindo:

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

3.3.2 - Atribuição automática de treinamentos para novos usuários;

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

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

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

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

3.3.7 - 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.

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

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

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

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

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

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

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

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

3.11. Permitir a emissão de certificados para os treinamentos.

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

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

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

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

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

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

3.15.3. Manter histórico por usuário e por campanha;

3.15.4. Permitir que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação.

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.

3.17. 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.

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

3.19. 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.

B. IMPLANTAÇÃO E SUPORTE

3.20. 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:

3.20.1. Acompanhar o projeto (programa de conscientização);

3.20.2. Esclarecer dúvidas;

3.20.3. Sugerir proativamente novos caminhos para o programa;

3.20.4. Ser ponte com o suporte técnico.

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

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

3.22. 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:

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

3.22.2. Configuração da integração com Active Directory e ADFS;

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

3.22.4. Habilitação de Duplo Fator de Autenticação.

3.23. 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*.

3.23.1. 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;

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

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

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

C. QUALIFICAÇÃO TÉCNICA E FINANCEIRA.

3.25. 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 **2.750 (dois mil e setecentos e cinquenta)** licenças de acesso à plataforma de conscientização ofertada, quantidade que representa 50% da demanda do Regional que solicita maior quantidade de licenças de acesso.

3.25.1. 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.

3.26. 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;

D. VIGÊNCIA E DOS PRAZOS

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) Passagem 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

Tab. 1 - Cronograma executivo

Todos os prazos em dias úteis. Havendo antecipação das entregas, os prazos posteriores são automaticamente antecipados.

E. 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.

4. IDENTIFICAÇÃO E COMPARAÇÃO DAS SOLUÇÕES ADERENTES AOS REQUISITOS

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) Software livre ou software público.

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

d) Solução de mercado, comercial.

Com base nos requisitos funcionais, em especial os requisitos de negócio estruturantes (fig 1), 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 plataforma 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)	3.1	Não (80)	Sim (486)	Sim (403)
	Conteúdo LGPD Nacional	3.1.2	Sim	Sim	Sim
	Entregar conhecimento através de conteúdos tais como: vídeos, games, quizzes, artes (posters), assessments (avaliações).	3.2	Sim	Sim	Sim
	Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior)	3.1.1	N/A	Sim	Sim
Conteúdo do Cliente	Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (Moodle, usado pela JE)?	3.5	Parcial/Não permite scorm	Sim	Não
	Todas as funcionalidades da plataforma aplicáveis ao conteúdo nativo são aplicáveis ao conteúdo da contratante inserido na plataforma?	3.5.1	Sim	Sim	Não
Implantação e Segurança	Possui integração com AD?	3.3.5	Sim	Sim	Sim
	Carga de usuários por meio de arquivos csv?	3.3.4	Sim	Sim	Sim
	Permite duplo fator de autenticação para usuários e administradores?	3.14	Não	Sim	Não
Normas de Segurança como conteúdo	Permite a inclusão dos normativos de segurança da contratante e o aceite pelos usuários? Formato PDF.	3.5 e 3.6	Não	Sim	Não
Automação	Atribuição automática de treinamento para novos usuários?	3.3.2	Não. A plataforma tem como base a gamificação.	Sim	Sim

			Funciona como um jogo.		
	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?	3.16	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?	3.12 e 3.19	Não	Sim	Sim
Gestão de Usuários e Cursos	Seleção de módulos de treinamento para grupo de usuários? (Atribuição de treinamentos).	3.3.1	Não	Sim	Sim
	Gestão de cursos, tais como: porcentagem de inscrições, cursos iniciados, incompletos, concluídos	3.8	Sim	Sim	Sim
	Acompanhamento online de progressão e desempenho dos usuários?	3.7	Sim	Sim	SIm
	Emissão de Certificados para os cursos?	3.11	Não	Sim	Sim
	Relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos?	3.10	Sim	Sim	Sim
	Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes?	3.3.3	Não, o administrador manda e-mails	Sim	Sim
	Inativação de usuários sem perda do histórico de dados?	3.3.6		Sim	Sim
	Disponibilizar perfis de acesso para gestão de campanhas e de treinamentos?	3.13	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?	3.9	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)?	3.3.7	Sim	Sim	Sim
Campanhas de Phishing	Permite a criação de número ilimitado de campanhas durante a vigência do contrato?	3.15.1	Sim	Sim	Sim
	Disponibiliza pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos pela contratante;	3.15.2	Sim	Sim	Sim
	Mantem histórico por usuário e por campanha	3.15.3	Sim	Sim	Sim
	Permite que os usuários seja testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação?	3.15.4	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.	3.17	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 3.20?	3.20, 3.21, 3.24	Sim	Sim	Sim
	Passagem de Conhecimento	3.23	Sim	Sim	Sim
Customização	Permite inserir a identidade visual da contratante nas	3.4	Sim	Sim	Sim

	campanhas e nas mensagens dirigidas aos usuários?				
Linguagem da Plataforma	Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br)	3.18	Sim	Sim	Não

Tabela 2 - Comparativo de soluções de mercado.

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

Item 3.1.1. 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.*

Item 3.14. 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:

1. Quais os usuários menos treinados na Justiça Eleitoral.
2. Quais usuários mais falharam nos testes de engenharia social.
3. Informações pessoais como nome, cpf, email e outras disponíveis na plataforma.

De posse dessas informações, o invasor poderia direcionar os ataques de engenharia social para esses usuários e ter sucesso em uma invasão à instituição.

Assim, é imprescindível que essa exigência voltada à segurança seja mantida pela Administração.

Item 3.17. Indicador de Maturidade em Segurança da Informação.

O Acórdão TCU Plenário 3143/2021 determina 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 ou milhares de usuários (no caso de alguns tribunais), não é razoável. Conforme já abordado neste Estudo, há necessidade de racionalizar a força de trabalho da Justiça Eleitoral, que já é muito reduzida, voltando o esforço do corpo de servidores para tarefas fins que não são passíveis de automação.

Item 3.19. APIs para exportação dos dados.

A própria redação do item já trás 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.

Itens de automação 3.3.2 e 3.16

3.3.2 - Atribuição automática de treinamentos para novos usuários;

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.

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.

Finalmente, transcrevo trecho do parecer do setor de Controle Interno desse Tribunal, no processo 9139/2006, referindo-se a Lei de Licitações:

“Inicialmente gostaríamos de destacar que a Lei de Licitações não veda o estabelecimento de cláusulas restritivas à participação no certame. Pelo contrário, a partir do momento em que a Administração define o objeto e as condições em que se dará a contratação, já está restringindo a participação na licitação das pessoas, físicas ou jurídicas, que atenderem aos requisitos previamente definidos.

O que se repele é a restrição despropositada, que não seja fruto das necessidades do interesse público a ser satisfeita.”

Segundo esta linha, a Equipe de Planejamento trouxe aos autos as justificativas referentes às principais cláusulas técnicas que restringiram a participação das plataformas pesquisadas.

O Estudo teve por base a comparação as principais soluções, mas a equipe de planejamento entende que diante da dinâmica do mercado, a lista pode não ser exaustiva. Há possibilidade de existirem outras plataformas que não foram analisadas. Assim, não obstante a Knowbe4 ser a única plataforma do estudo que atende integralmente as exigências, o Termo de Referência não trará indicação de marca, apresentando somente as necessidades da Administração. Isso permitirá ainda que todos os players do mercado possam trazer questionamentos que julgarem pertinentes a respeito de qualquer uma das especificações constantes no Termo.

Cabe ressaltar finalmente que, mesmo sendo a Knowbe4 a única a atender os requisitos, há no mercado várias empresas que fornecem a solução, permitindo, assim, um certame competitivo.

5. INDICAÇÃO DA STIC ESCOLHIDA

Solução de mercado, comercial.

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

DESCRIÇÃO DA SOLUÇÃO

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

ESTIMATIVA DE PREÇO

O custo unitário de cada licença de acesso, considerando o volume de 25.730 licenças de acesso é de R\$ 119,80.

JUSTIFICATIVA/MOTIVAÇÃO DA ESCOLHA

Conforme item 1.2 deste estudo.

ADERÊNCIA AOS REQUISITOS

Importante demonstrar que os requisitos tecnológicos que irão compor o Termo de Referência estão plenamente alinhados às necessidades da área demandante expressas através dos requisitos funcionais. A tabela abaixo lista cada uma das exigências agrupadas em temas, indicando os requisitos funcionais que as originaram.

Tema	Característica	Requisito Funcional Originário	Requisito Tecnológico
Conteúdo Nativo	Conteúdo em língua portuguesa ou legendado em português nacional (300 itens)	2.1, 2.15	3.1
	Conteúdo LGPD Nacional	2.1	3.1.2
	Entregar conhecimento através de conteúdos tais como: vídeos, games, quizzes, artes (posteres), assessments (avaliações).	2.2	3.2
	Plataforma/Conteúdo em conformidade com padrão WCAG (versão 2 ou superior)	2.11	3.1.1
Conteúdo do Cliente	Permite carga de treinamentos da contratante, incluindo os formatos de vídeo e SCORM (Moodle, usado pela JE)?	2.3	3.5
	Todas as funcionalidades da plataforma aplicáveis ao conteúdo nativo são aplicáveis ao conteúdo da contratante inserido na plataforma?	2.3	3.5.1
Implantação e Segurança	Possui integração com AD?	2.8	3.3.5
	Carga de usuários por meio de arquivos csv?	2.8	3.3.4
	Permite duplo fator de autenticação para usuários e administradores?	2.19	3.14
Normas de Segurança como conteúdo	Permite a inclusão dos normativos de segurança da contratante e o aceite pelos usuários? Formato PDF.	2.5	3.5 e 3.6
Automação	Atribuição automática de treinamento para novos usuários?	2.9	3.3.2
	Criação automatizada de um programa personalizado em segurança da informação ou fazer recomendação automática de treinamentos, considerando, no mínimo, o nível de risco em segurança da informação dos usuários?	2.9	3.16
	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?	2.20	3.12 e 3.19

Gestão de Usuários e Cursos	Seleção de módulos de treinamento para grupo de usuários? (Atribuição de treinamentos).	2.7 e 2.9	3.3.1
	Gestão de cursos, tais como: porcentagem de inscrições, cursos iniciados, incompletos, concluídos	2.7	3.8
	Acompanhamento online de progressão e desempenho dos usuários?	2.7	3.7
	Emissão de Certificados para os cursos?	2.7	3.11
	Relatórios executivos e de gestão sobre as campanhas e resultados de treinamentos?	2.7	3.10
	Disparo automático de e-mails de lembrete para usuários com treinamentos pendentes?	2.7	3.3.3
	Inativação de usuários sem perda do histórico de dados?	2.7	3.3.6
	Disponibilizar perfis de acesso para gestão de campanhas e de treinamentos?	2.7	3.13
	Provê ambiente de gestão que possibilita a criação de grupos de usuários com base em comportamento frente às simulações e treinamentos realizados?	2.7	3.9
Campanhas de Phishing	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)?	2.7	3.3.7
	Permite a criação de número ilimitado de campanhas durante a vigência do contrato?	2.4	3.15.1
	Disponibiliza pelo menos 50 modelos de campanhas em português e permitir a personalização dos modelos pela contratante;	2.4	3.15.2
	Mantém histórico por usuário e por campanha	2.4	3.15.3
Indicador de Maturidade em Segurança	Permite que os usuários seja testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação?	2.4	3.15.4
	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	2.6	3.17
Supporte 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?	2.14	3.20, 3.21, 3.24
	Passagem de Conhecimento	2.10	3.23
Customização	Permite inserir a identidade visual da contratante nas campanhas e nas mensagens dirigidas aos usuários?	2.12	3.4
Linguagem da Plataforma	Disponibilizar ambiente operacional para alunos e administradores totalmente em língua portuguesa (pt-br)	2.13	3.18

Tabela 3 - Alinhamento entre requisitos funcionais e tecnológicos.

RELAÇÃO ENTRE DEMANDA PREVISTA E A STIC

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
TRE/AC	179	Ofício 27/2022 - PRESI/DG/GADG
TRE/AL	483	Ofício 790/2022 - TRE-AL/PRE/DG/GDG
TRE/AP	260	Ofício 519/2022 - TRE-AP/PRES/DG/GAB-DG
TRE/BA	2000	Ofício 1588/2022 - PRE/DG/ASSESD
TRE/CE	1650	Ofício 464/2022
TRE/DF	350	Ofício nº 606 / 2022 - TRE-DF/PR/DG/GDG
TRE/ES	520	Processo SEI 0001048-53.2022.6.08.8000
TRE/GO	1150	Ofício 46 - DG
TRE/MA	700	Ofício 1754/2022 - TRE-MA/PR/DG/STIC/GABSTIC
TRE/MG	500	Ofício 532/2022 - DG Ofício 696/2022 - DG (retificação)
TRE/MS	600	Despacho 7655/2022 - TRE/PRE/DG/AEDG
TRE/MT	700	Ofício 23/2022
TRE/PA	600	Ofício 1333/2022 - CSI
TRE/PB	800	Ofício 51/2022 - TRE-PB/PTRE/DG
TRE/PI	765	Ofício 39/2022 - TRE/PRESI/DG
TRE/PR	1500	Ofício 324/2022 - GABDG
TRE/RJ	2373	Ofício DG 47/2022
TRE/RN	500	Ofício 48/2022 - DG
TRE/RO	400	Ofício 53/2022 - PRES/DG/GABDG
TRE/RR	200	Ofício 511/2022 - TRE-RR/PRES/DG/GabDG
TRE/SC	1100	Ofício DG/GAB n. 216/2022
TRE/SE	300	Ofício TRE-SE 1410/2022 - GAB-DG
TRE/SP	5500	Ofício TRE-SP n. 449/2022
TRE/TO	600	Ofício 1044/2022 - PRES/DG/STI/CSI/SERES
TSE	2000	Ofício GAB-DG nº 1197/2022
TOTAL	25730	

Tabela 4 - Demanda dos Tribunais

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

TIPO	TOTAL
ESTAGIÁRIOS	31
EFETIVOS	313
REQUISITADOS	100
TERCEIRIZADOS	38
REMOVIDOS PARA TRE-ES	17
SEM VÍNCULO EFETIVO	7
MEMBROS ATIVOS	12
LOTAÇÃO PROVISÓRIA	2
	520

Tabela 5 - 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 referida ARP não deve ser aberta para participação de outros órgãos, tendo em vista que:
 - Os Tribunais Eleitorais foram consultados, informando o quantitativo de licenças e formalizando sua participação no certame desde a origem.
 - Os pilares do programa de conscientização que originaram as especificações técnicas deste Estudo foram definidos por grupo nacional constituído pelo TSE, não cabendo ajustes para outros órgãos.

- O cronograma de execução da contratação previsto pelo Tribunal Superior Eleitoral, remetido a este TRE/ES e registrado no processo SEI 0002446-35.2022.6.08.8000 seria exíguo para quaisquer ajustes.
- A equipe entende que a ARP não deve ser aberta para adesão (caronas), também em função de tratar-se de objeto definido para as necessidades da Justiça Eleitoral.

6. INDICAÇÃO DA NECESSIDADE DE ADEQUAÇÃO AMBIENTAL

Plataforma em Nuvem - Não há necessidade de Adequação Ambiental

ANÁLISE DE RISCOS

7. IDENTIFICAÇÃO DOS PRINCIPAIS RISCOS

FASE DE CONTRATAÇÃO

1 - ATRASO NO TRÂMITE PROCESSUAL

FASE DE EXECUÇÃO

2 - EXPOSIÇÃO DE INFORMAÇÕES DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO

3 - INEXECUÇÃO CONTRATUAL

4 - BAIXA PARTICIPAÇÃO NOS TREINAMENTOS

IDENTIFICAÇÃO DOS RISCOS DE DEPENDÊNCIA TECNOLOGICA

Os riscos de dependência tecnológica e o tratamento compõem o **item 3.E.** deste Estudo.

8. RELAÇÃO DOS RISCOS E AÇÕES DE MITIGAÇÃO

ANÁLISE DOS RISCOS

8.1. Probabilidade e impacto, ações de prevenção/contingência, responsáveis. Incluídos nas tabelas abaixo.

FASE DE CONTRATAÇÃO

EVENTO 1 - ATRASO NO TRÂMITE PROCESSUAL

Causa	Efeito	Probabilidade	Impacto
Inadequação dos aspectos técnicos do TR ao mercado, Inadequação dos aspectos administrativos do TR à expectativa da administração	Não efetivar treinamentos de usuário em Segurança da Informação antes da Eleição de 2022	Baixo	Médio

Plano de Resposta - Ações	Responsável
1 - Consultar empresas do ramo sobre adequação das especificações técnicas às características dos equipamentos fornecidos pelo mercado.	Integrante Técnico
2 - Verificar/adequar/sugerir questões sobre os aspectos administrativos da contratação	Integrante administrativo
3. Aplicar treinamentos avulsos voltados a Segurança da Informação	STI e SGP

FASE DE EXECUÇÃO**EVENTO 2 - EXPOSIÇÃO DE INFORMAÇÕES DE MATURIDADE EM SEGURANÇA DA INFORMAÇÃO**

Causa	Efeito	Probabilidade	Impacto
Comprometimento de credenciais de administradores da plataforma	Uso das informações para ações de engenharia social visando comprometer a infraestrutura tecnológica	Baixa	Alto

Plano de Resposta - Ações	Responsável
1 - Inserir no termo de referência a necessidade de duplo fator de autenticação para acesso à plataforma	Integrante Técnico

EVENTO 3 - INEXECUÇÃO CONTRATUAL

Causa	Efeito	Probabilidade	Impacto

Indisponibilidade intransponível na plataforma	<ul style="list-style-type: none"> - Interrupção do Programa de treinamento continuado. - Indisponibilidade das informações gerenciais de maturidade. 	Baixo	Médio
--	---	-------	-------

Plano de Resposta - Ações	Responsável
1 - Inserir no termo de referência a necessidade de APIs para exportação dos dados gerenciais.	Integrante Técnico

EVENTO 4 - BAIXA PARTICIPAÇÃO NOS TREINAMENTOS

Causa	Efeito	Probabilidade	Impacto
Gestão inapropriada da condução do programa de treinamento.	Baixo crescimento da maturidade em Segurança da Informação	Média	Alto

Plano de Resposta - Ações	Responsável
1 - Integrar as equipes de TIC e SGP na gestão do programa e da plataforma contratada	Fiscais Técnicos (SGP e STI)
2. Buscar Apoio da Alta Administração para aprovação de um cronograma de execução de treinamentos para todos os usuários.	SGP e STI
3. Criar equipe Nacional para elaboração de um programa padrão com base na plataforma que poderá ser usado por todos os Tribunais.	TSE

ANÁLISE DE SUSTENTAÇÃO DO CONTRATO

9. RECURSOS MATERIAIS E HUMANOS

9.1. 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 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 a construção do programa de capacitação em Segurança da Informação;
- 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.

9.2. 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.

Como está sendo contratada uma plataforma única para toda a Justiça Eleitoral, uma solução viável para conduzir o programa seria a formalização de uma comissão nacional, com participação das áreas de recursos humanos e tecnologia da informação, visando a elaboração de um cronograma de treinamentos e testes que poderia ser usado por todos os Tribunais que tivessem interesse. Essa ação otimizaria os recursos humanos e contribuiria para uma evolução de maturidade similar em toda a justiça eleitoral.

10. DESCONTINUIDADE DO FORNECIMENTO

Conforme Item 3.E deste estudo, todas as informações gerenciais devem ser exportadas ao longo do contrato para continuidade do programa de conscientização no caso de descontinuidade do fornecimento.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO (Portaria DG nº 82 (0712224))

Integrantes Demandantes SANDRO MERÇON DA SILVA (substituto: OLGA BAYERL VITA)

Integrantes Técnicos pela área de Tecnologia da Informação OLGA BAYERL VITA (substituto: SANDRO MERÇON DA SILVA)

Integrantes Técnicos pela área de Gestão de Pessoas: DANIEL FLÁVIO DE OLIVEIRA GONZAGA (substituta: ARIANY TEIXEIRA DA MOTTA NICCHETTI)

Integrante Administrativo JOSE ADRIANI BRUNELLI DE STEFFANI (substituto: CARLOS ALBERTO DA ROCHA PADUA FILHO)

GRUPO NACIONAL DE PLANEJAMENTO DA CONTRATAÇÃO

TRE-ES / TRE-GO / TRE-TO / TRE-DF

Vitória, 09 de junho de 2022.



Documento assinado eletronicamente por **OLGA BAYERL VITA, Técnico Judiciário**, em 09/06/2022, às 11:41, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **JOSE ADRIANI BRUNELLI DE STEFFANI, Secretário(a)**, em 09/06/2022, às 11:46, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **SANDRO MERÇON DA SILVA, Coordenador(a)**, em 09/06/2022, às 11:52, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **DANIEL FLAVIO DE OLIVEIRA GONZAGA, Chefe de Seção**, em 09/06/2022, às 12:41, 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 **0751472** e o código CRC **AF9F31CF**.

